

A CONCEPTUAL FRAMEWORK OF INFORMATION SECURITY DATABASE
AUDIT AND ASSESSMENT IN UNIVERSITY BASED ORGANIZATION

MUNEEB UL HASAN

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

MAY 2018

In the name of ALLAH, the Most Gracious and the Most Merciful
To my beloved father and to my beloved mother may ALLAH bless them both who
made me see further by standing on their shoulders, and to all my family and friends.
Thank you.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor **Dr. Siti Hajar Othman** for his constant support during my study at UTM. She inspired me greatly to work in this project. Her willingness to motivate me contributed tremendously to our project. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

Last but not the least, deepest gratitude goes to my beloved family members for their endless love, prayers and encouragement and to everyone who has been involved in this project even by coincidence.

ABSTRACT

Today, databases are one of the most important things in the IT world and it is also becoming more popular and organizations globally are gradually moving their traditional IT setup to database model to gain the benefits of securing the data and in terms of providing easy access and elasticity of IT services. With database security, the IT service roles within an organization become integrated hence giving the overall IT operating model a more structured layout. Such objectivity however can only be materialized when proper planning and execution are put in place. As such, a proper execution and implementation of database system would include a stringent set of checks and audit processes. The problem is like every database is having right now is there information records that needs to be secured and the information assets and more private records need to be secured. A conceptual Information Security Database Audit and Assessment framework (ISDAA) will enhance to identify the best approach to audit and assess only the information assets through information security database audit. The goal of database auditing is central towards determining if the services engaged are meeting certain legal requirements in terms of protecting customer's data and organization standards to achieve secure data assets success against various security threats. Therefore, this project has a conceptual framework which will be developed from previous frameworks through literature review and after that the variables influencing the auditing of database from those previous frameworks such as access control, oracle database control, SQL(DML), Object(DDL) and IT audit quality will be used for the audit process. After this The method that will be used to collect the data by these variables for enhancing the framework will be by comparing it with other frameworks with expert reviews from CICT UTM data center and IT department experts and then formulate an updated framework which has the following enhanced components such as DB log, DB Client, DB API and Alerting and Monitoring.

ABSTRAK

Hari ini, pangkalan data adalah salah satu perkara yang paling penting di dunia IT dan ia juga menjadi lebih popular dan organisasi di seluruh dunia secara beransur-ansur memindahkan persediaan IT tradisional mereka kepada model pangkalan data untuk mendapatkan faedah mendapatkan data dan dari segi menyediakan akses mudah dan keanjalan perkhidmatan IT. Dengan keselamatan pangkalan data, peranan perkhidmatan IT di dalam organisasi menjadi terintegrasi dengan itu memberikan model operasi IT keseluruhan susun atur yang lebih berstruktur. Objektivitas semacam itu hanya dapat dijadikan kenyataan apabila perancangan dan pelaksanaan yang tepat dilaksanakan. Oleh itu, pelaksanaan dan pelaksanaan sistem pangkalan data yang tepat akan merangkumi satu set pemeriksaan dan proses audit yang ketat. Masalahnya seperti setiap pangkalan data yang ada sekarang terdapat rekod maklumat yang perlu dijamin dan aset maklumat dan lebih banyak rekod peribadi memerlukan untuk diamankan. Rangka kerja Audit dan Penilaian Pangkalan Data Keselamatan Maklumat (ISDAA) akan meningkatkan untuk mengenal pasti pendekatan terbaik untuk mengaudit dan menilai hanya aset maklumat melalui audit pangkalan data keselamatan maklumat. Tujuan pengauditan pangkalan data adalah penting untuk menentukan sama ada perkhidmatan yang terlibat memenuhi undang-undang tertentu keperluan dari segi melindungi piawai data dan organisasi pelanggan untuk mencapai kejayaan aset data yang selamat terhadap pelbagai ancaman keselamatan. Oleh itu, projek ini mempunyai kerangka konseptual yang akan dibangunkan dari kerangka sebelumnya melalui kajian literatur dan selepas itu, pembolehubah yang mempengaruhi pengauditan pangkalan data dari kerangka sebelumnya seperti kawalan akses, kawalan database oracle, SQL (DML), Object (DDL) dan kualiti audit IT akan digunakan untuk proses audit. Selepas ini Kaedah yang akan digunakan untuk mengumpul data oleh pemboleh ubah ini untuk meningkatkan rangka kerja adalah dengan membandingkannya dengan rangka kerja lain dengan ulasan pakar dari pusat data CICT UTM dan pakar jurusan IT dan kemudian merumuskan rangka kerja yang dikemas kini yang mempunyai peningkatan berikut komponen seperti log DB, DB Client, API DB dan Alerting dan Pemantauan.

TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATION	xii
	 LIST OF APPENDICES	 xiii
1	INTRODUCTION	1
	1.1 Overview	1
	1.2 Problem Background	2
	1.3 Problem Statement	4
	1.4 Aim of the Project	4
	1.5 Objectives	5
	1.6 Scope of the Project	5
	1.7 Significance of the Project	6
	1.8 Report Organization	7
	1.9 Summary	8

2	LITERATURE REVIEW	9
2.1	Introduction	9
2.2	Database Audit	10
2.3	Information Security Framework	13
2.3.1	COBIT Framework	14
2.3.2	COSO Framework	16
2.4	Database Security Audit Framework	17
2.4.1	Integrigy Framework for Database Audit	17
2.4.1.1	Integrigy Framework for Auditing of Database	18
2.4.2	Database Auditing for Oracle Database	20
2.5	Information Security Audit and Assessment Components	22
2.5.1	Preparation Phase	22
2.5.2	Performance Phase	23
2.5.3	Conclusion Phase	23
2.6	IT Audit the analysis and impact of IT audit quality	24
2.7	Internal Audit Process Quality	27
2.8	Previous Framework Components on Database Audit	35
2.9	IT Information Assets	40
2.10	University Based Organization	43
2.10.1	UTM (CICT)	43
2.11	Summary	44
3	RESEARCH METHODOLOGY	45
3.1	Introduction	45
3.2	Research Operational Framework	46
3.3	Project Phases	49
3.3.1	Phase 1: Research Problem Definition	49
3.3.2	Phase 2: Design Phase	50
3.3.2.1	Data Collection	51
3.3.3	Phase 3: Analysis of Findings Phase	53
3.4	Summary	54

4	DESIGN AND IMPLEMENTATION	55
4.1	Introduction	55
4.2	Initial Proposed Conceptual Framework	55
4.3	Oracle Database Controls	58
4.3.1	Object(DDL)	59
4.3.2	SQL (DML)	59
4.4	Access Control	61
4.5	Alerts, Report and IT Audit Quality	62
4.6	Summary	63
5	RESULTS AND DISCUSSION	64
5.1	Introduction	64
5.2	Validation Technique 1: Comparison against other models	64
5.2.1	Against the challenges of Data Quality and assessment in database	65
5.2.2	Against Integrity Framework for Database Auditing	67
5.2.3	Against Overview of Database Auditing Framework	70
5.2.4	Against a Framework for Database Audit and Control Flow Checking for a Wireless Controller	73
5.2.5	Against a Practical Database Framework for Intrusion Detection System	75
5.2.6	Against Database Auditing for Oracle Database	78
5.3	Comparing Concepts in Framework of V1 against ISDAA	81
5.4	Expert Review and justification of the enhanced components	82
5.5	Enhanced Information Security Database Audit and Assessment Framework	84
5.6	Summary	86

6	CONCLUSION & FUTURE WORK	87
6.1	Introduction	87
6.2	Overview	87
6.3	Project Achievement	88
	6.3.1 Framework for Information Security Audit	88
6.4	Project Shortcomings and Constraints	89
6.5	Concluding Remarks	89
6.6	Summary	90
	REFERENCES	91
	APPENDIX A	93

LIST OF TABLES

FIGURE NO.	TITLE	PAGE
2.1	14 Key Security Events	22
2.2	Importance of IT Audit Factors on Audit Quality	28
2.3	Audit Process Quality	31
2.4	Comparison of Previous frameworks	36
2.5	Table of questions of define assets	41
3.1	Summary Phase of Research Methodology	48
5.1	Quality Assessment of big data Support Concepts in Database Security Audit Framework	67
5.2	Integrigy Framework for Database Auditing Concept Supports the ISDAA Concept	69
5.3	Overview of Database Auditing Framework Concept Support the ISDAA Concept	72
5.4	Database Audit Framework for Control Flow Support Concept of ISDAA	74
5.5	Database Framework IDS Support Concept of ISDAA	76
5.6	A Comparison Between Integrigy Framework Concept and ISDAA Concept	78
5.7	Comparing Concepts in Frameworks V1 against ISDAA Concepts	81
5.8	Expert Reviews	82
5.9	Audit Process Relationship	85

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Database Audit System Architecture	12
2.2	Audit Process	15
2.3	COSO Expanded Cube	16
2.4	Integrigy Framework Methodology for Database Audit	18
2.5	Integrigy Framework for Auditing and Logging	19
2.6	A Conceptual Framework	21
2.7	Auditing Phases	22
2.8	A Theoretical Framework for Internal Audit Process	28
2.9	Example of Information Assets	41
3.1	Operational Framework	45
3.2	A Theoretical Framework for Internal Audit Process	48
4.1	Initial Proposed Conceptual Database Framework	55
5.1	Quality Audit Assessment of Big Data in Database	63
5.2	Integrigy Framework for Database Auditing	65
5.3	Overview of Database Auditing Framework	69
5.4	Audit Process	71
5.5	Deployment of the DIDS	73
5.6	Architecture of the DIDS	74
5.7	Integrigy Framework for Auditing and Logging for Database	76

LIST OF ABBREVIATION

AC	-	Access Control
IAQ	-	IT Audit Quality
IT	-	Information Technology
IS	-	Information Security
SQL	-	Structured Query Language
O	-	Object
ODC	-	Oracle Database Control

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Comparison Table	93

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the 21st century, we have a digital era in which we find that the organization nowadays are somehow linked with the information and the strategy like how they will keep or manage the organizations information. In all the cases protection of database is a very important priority of information systems organizations. Database are the main aspect that are behind every system that effects almost every aspect of our lives that are bank accounts, academic assets, medical records and phone records. The security of database systems can be defined by the implementation of authentication, access control, identification and other related measures. (L. Liu, 2009)

The purpose of the database audit is to ensure that record every access to the database more effectively and immediately, generate the detailed analysis of the system record, so that the database system can use the five elements to record every incident; when, who, where, what, how (Anon., 2014). Information security database audit is part of an investigation for auditing and monitoring policies of the organization that is being audit e.g. UTM (CICT).

A conceptual information security framework is an analytical tool with several variations and contexts. It is used to make conceptual distinctions and organize ideas about the security of information regarding any field. Information Security audit and assessment is a systemic way for measuring technical assessment of how the organizations security policy is employed. It is part of the on-going process of defining and maintaining effective security policies. The audit subsystems which are in the commercial database system allow to have a detailed information about the database users, database objects and operations on the data should be highly observed and the information which is being taken by the audit. The database Audit should not only secure the database but also the organization itself so that it can perform tasks risk free.

1.2 Problem Background

In information security, the traditional database mechanism systems such as data encryption and access control are basically useless by a trusted employee who has or can easily obtain the right credentials to the data that is stored in that database. To add to this more enterprise are getting the databases access, such as HR manager, database administrators, application developers and even software engineers. If an enterprise has not done auditing or monitoring of their databases, then their valuable assets are at very high risk because their important assets can be compromised or even get stolen by some attacker. (L. Liu, 2009).

There have been many number of proposed solutions for database security for e.g Vanhor states that embedding a monitoring and auditing system in databases makes it easy to take and implement security policies on organizations. Using a database audit can be very helpful in protecting the transaction logs of the database system. However, storing these logs may cause some serious storage and performance problems (O. Cinar, 2017).

The market nowadays has a very wide range of products for database security audit systems for e.g. Domestic manufacturers have the same products for security audit function as they all have problems and defect. There are some modules which are known as Plug-in modules which are embedded in the database management system and they are also widely used in database vendors because these things can deal with the internal processing and can control it more accurately. But among these products they do not usually fit for others, therefore they cannot provide a good support in the database environment. So, basically the problem facing here is that there are a lot of models and frameworks that has described that data sets in the database can be saved but the big issue is that no framework has clearly defined the main problem for databases in University Organization. (Anon., 2014).

In the industry, big data awareness is increasing day by day. Currently the most widely used method of database audit is based on a log (Matt Bishop,1990). The relationship between big data and database audit system is the data itself which needs to be protected to have less disasters. The three steps involving audit process are: a) Audit analysis, b) data collection and c) result output. From these steps audit analysis is the most important but also the weakest step. The audit content has the great difference between the actual operation of the system and the model design in the process of database audit, for example the problem of low audit efficiency. In the process of database audit, when faced with huge data records the organizations which browse through the data is analyzed manually which will not be able to dig out good users and reflect the value of data (J. Shi, 2016). In Academia side focusing universities there is almost no auditing of database research. Universty database is also very important as it has many important assets that need to be protected.

1.3 Problem Statement:

In recent times cybercrime is getting vast in the academics. There are some risks that hit the university assets which are basically stored in a database that is very important as an information and that can leave to many malicious activities. *The problem is like every database is having right now is there information records that needs to be secured and by the problem background as describe in part 1.2 it clearly says that the information assets and more private records need to be secured.* A conceptual framework will enhance university management to identify the best approach to audit and assess only the information assets through information security database audit. By understanding how to proceed auditing of database through the related Information security frameworks so that this information may help how to do the audit in a secure manner and to have all the information of the database auditing and also by making the quality of audit more effective. It is especially important for a institute of higher learning such as in Universiti Teknologi Malaysia (UTM) through its computer centre called the Center for Information and Communication Technology (CICT). The rest of this thesis will use CICT, UTM as an abbreviation of this center.

1.4 Aim of the Project:

This project will help in making a better audit experience for the staff of the related university by improving the information security decision making in areas like audit, assessment and risk management. The developed conceptual information security database audit and assessment framework will improve the security of private information in databases by following the proposed conceptual framework

and it will help on technical bases as well. By applying this framework in CICT, UTM the auditing of the databases will be the key to secure the university Assets and to make the audit quality better for information systems for the betterment of the related university in coming years.

1.5 Objectives of the Project

The objectives of this project are mentioned as follows:

1. To Analyze variables which are affecting the security audit and assessment quality for database audit system.
2. To propose a conceptual information security framework for database audit and assessment.
3. To evaluate the proposed security conceptual framework by comparison with other related frameworks.

1.6 Scope of the Project:

The scope of this project is it take the CICT, UTM as a case study. The research leveraged UTM huge research contribution in term of resource, facility, data, paper, journal, and ideas from all the relevant faculty and departments until the end of the research.

Most of the information will be contributed by the previous research on Information Security frameworks like COBIT and COSO that has been done from different domains and areas. Experts from IT security domain will also help in getting the right results.

University-based organization such as CICT, UTM will be case study in this research. The methods used in this research will be comparison of the initial framework with other frameworks.

1.7 Significance of the Project:

This project will help in making a better framework by improving the information security decision making in areas like audit, assessment and risk management. IT auditors will feel relaxed to work or audit any information regarding databases in universities because this research will be assisting them with every information they need to know to do the Audit so that no one will have less information about the databases. This framework is the key to secure the databases and information systems for the betterment of the related university in coming years. This framework will also verify that policies and procedures are in place. It will also ensure access to the operating system is properly restricted. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need.

Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change. The enhancement of this framework after comparison will affect security level of the information systems that are in the university and it will make a risk-free environment in all parts of the faculty.

1.8 Report Organization

This thesis has five chapters. To accelerate understandings to the thesis, a brief overview of the contents of each chapter are as follows:

Chapter 1 discuss on the introduction of the research and serves as a road map to reader through brief description on the contributions of this thesis.

Chapter 2 discuss on the literature Review for this study against previous related publications. This includes the reviews of research related to the method and process of database auditing and its assessment and the audit quality of the database and domain of interest, the information security audit and assessment.

Chapter 3 provides the discussion on research methodology used on this thesis which are Planning Phase, Design Phase and Analysis of Finding Phase. Through those phases, some of the processes involved are such framework collections, extraction of general concepts, shortlisting the candidate definitions.

Chapter 4 explains the design of the implementation on the database audit by the help of the conceptual framework which has initially 5 main components: i) Access Control, ii) IT Audit Quality, iii) Object (DDL), iv) SQL (DML) and v) Oracle Database Controls.

Chapter 5 provides the conclusion, contributions, and summarizes of the research outcome such as works that have been done to accomplish the research objective and concludes with recommendations for futures research relevant to this thesis.

1.9 Summary

In conclusion, this chapter mainly discussed about the preliminary information about the research. Problem background and research aim is pointed out for reader to have a better understanding on the reason this research are needed. Besides that, the objectives, research scope, and research contribution are also provided to clear information on areas that been focussed on this thesis. In the next chapter, literature review of the thesis will be elaborate, discuss, and analysis of the relevant thesis framework.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction:

In the 21st century, we have a digital era in which we find that the organization nowadays are somehow linked with the information and the strategy like how they will keep or manage the organizations information. In all of the cases protection of database is a very important priority of information systems organizations. Database are the main aspect that are behind every system that effects some part of our life that are accounts of bank, academic assets, records of medical and phone records. The security of database systems can be defined by the implementation of authentication, access control, identification and other related measures (Lianzhong Liu, 2009).

The database audit is basically to ensure that to get the most efficient amount of record which have almost all the detailed access for the database which will be effectively and immediately generate all the detailed analysis of the system record, for which we will have these five elements when the database system is being audited;- when, who, where, what, how (Kehe Wu, 2014). Information security database audit is part of an investigation for auditing and monitoring policies of the organization that is being audited e.g. UTM administrative systems and CICT.

A **conceptual framework** is an analytical tool with several variations and contexts. It is used to make conceptual distinctions and organize ideas. Strong conceptual frameworks capture something real and do this in a way that is easy to remember and apply. The proposed framework in 4.1 will show a broad and technical view about the information security conceptual framework for database audit and its assessment. The technical reason of using a conceptual framework for this area is because it will show the systematic way of the whole process and the working hypothesis that will show that the framework is actually applicable in the for the database audit and its assessment. If the framework is not conceptual in the database audit, then the audit phases will not be properly described and also the framework will be not sufficient to be called a conceptual framework.

Information Security audit and assessment is a systemic way for measuring technically how the organizations security is employed and the policy. It is a process of defining and getting maintained for effective security policies. The audit subsystems which are in the commercial database system allow to have a detailed information about the database users, database objects and operations on the data should be highly observed and the information which is being taken by the audit. The database Audit should not only secure the database but also the organization itself so that it can perform tasks risk free.

2.2 Database Audit

Auditing is a very special tool nowadays basically of all the data breaches for forensic analysis. All actions that take place when the audit is being done is by the database administrator. This is a practice that will detect disasters and suspicious activities inside the database which enables the DBA to take further actions (Reena R. Chaudhari, 2015).

Database auditing involves observing a database so to be aware of the database users. Database are the main reason that are behind every system that will affect most of every aspects of our lives – that will be our bank accounts, phone records, medical records, employment records almost everything that has information of significance in our lives is maintained by a modern database management system. If the database system, that we intent to implicit our most sensitive data is not secured then the potential impact in our lives and even our border society, could be equal to devastating results.

The implementation of user identification, authentication, access control and other measures, the security of the database system can be elevated. But the main problem is the database is far from secure because these implementations and measures are not capable of monitoring and logging database activities, which can be helpful when an audit is done of a system from a secure standpoint.

The only solution which we have to this problem is implementing database auditing. Security and data center teams must be sharp enough to implement and enforce a set of best practices to address the insider threats. IT architects must then bolster the policies by using database auditing rather than other security features that has been built into other major database platforms (Lianzhong Liu, 2009).

Implementing security policies that will ensure high-level overview and meet business goals will depend on database security. The policies of security can be implemented using access control rules. Access control is one of the most important components of databases security. Access control has three major classes: Discretionary access control (DAC), Mandatory access control (MAC) and Role-based access control (RBAC). DAC policies works when the requestors identity is based on control access and it is basically with access rules saying what requestors are or are not allowed. MAC policies control accesses by the help of a central authority which is basically based on mandated regulations. RBAC policies control accesses will depend on the role of users who are within the system and on the rules,

which states that what accesses are users actually allowed in the given rules (Yang, 2009)

Database auditing systems contains two important parts: 1) Web management platform and 2) protocol analysis module. In this the second part which is protocol analysis module can be further subdivided into six parts which are: Network Data Capture module, TCP/IP data processing module, configuration module, strategic matching module, protocol processing module, SQL statement analysis module. Fig 2.1 shows the database auditing system design (Kehe Wu, 2014)

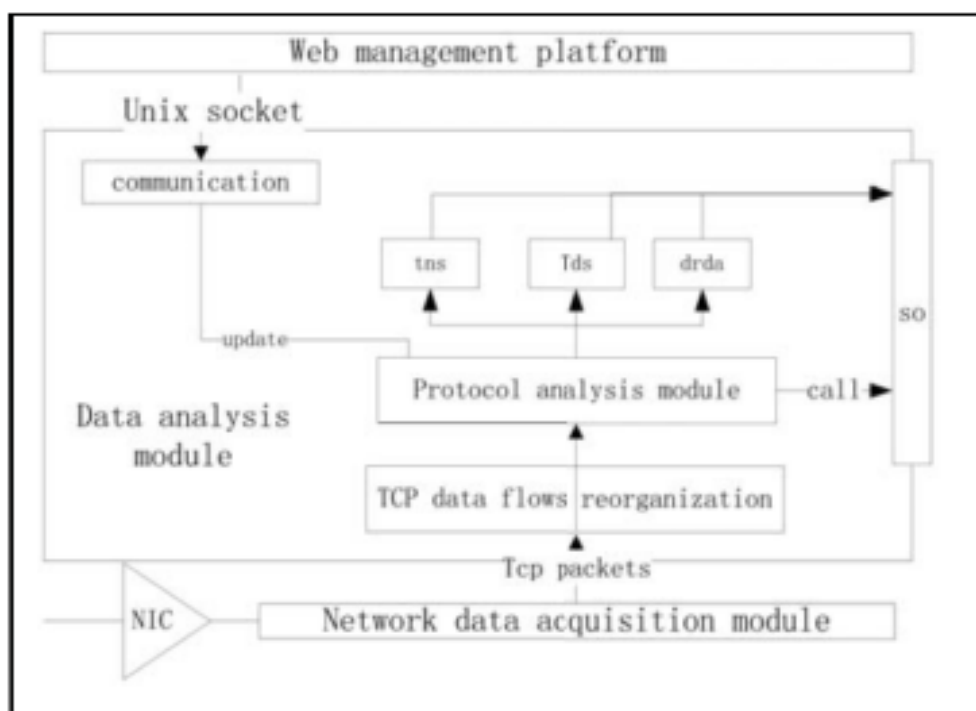


Figure 2.1: Database audit system architecture

The market nowadays has a very wide range of products for database security audit systems. Domestic manufacturers have the same products for security audit function as they all have problems and defects. There are some modules which are

known as Plug-in modules which are embedded in the database management system and they are also widely used in database vendors because these things can deal with the internal processing and can control it more accurately. But among these products they don't usually fit for others, therefore they cannot provide a good support in the database environment (Kehe Wu, 2014)

In the industry, big data awareness is increasing day by day. Nowadays the methods which are being used very often for database audit are all based on logs which are previously well described by Matt Bishop in 1990. The three steps which involve audit process are: Audit analysis, data collection with all the output results and from these steps the analysis of the audit is the most important and also the weakest step. Basically, the audit content has a very big difference between two of the most important things that is the actual operation of the system and the model design in the process of the database audit. When the process of database audit starts it faces huge amount of data records for enterprise and /organizations which will be browse through the data when it is analyzed manually, and it will not be able to take out the best users and bring useful data (Jia Shi, 2016).

2.3 Information Security Framework

An Information security framework is adopted which is taken in a broad or non-technical view. Cyber security is a difficult, ever evolving problem and a holistic overview in a way which is to provide a security framework in which it is to involve the research which being done. Right now, security dilemmas include: the pored habitation of information security software is continually upgraded and the sophisticated malware production and management; and the mistrust between different communities, and the aggressive nature of cyber security protection (Fielden, 2010).

The Oxford dictionary 1983 clearly describes a framework which is structured with the contents that have been put under some circumstances and which can be related further to thoughts which are directed for a reason. Information assets regarding employee behavior is very important in this society. Many people do not understand this term.

The standards of the Information security audit frameworks that will be used are as follows: a) COBIT Framework and b) COSO Framework. These two types of IS frameworks are mostly used for IT, auditing and governance. Section 2.3.1 and 2.3.2 describe the description of COBIT and COSO. Also, explain on the relationships of the models with information security audit and assessment.

2.3.1 COBIT Framework

COBIT is an organization which basically has a range of frameworks, standards and some documents that are all related to IT, and their primary goal is to focus on the alignment of COBIT'S use in the IT world with all the achievements that will be done for the organizational goals. COBIT is a very comprehensive framework which includes thirty-four different control objectives which are all developed by forty-one international source documents and as well as the documents are validated internationally so that they can help balance the risk against investment in IT controls. The control objectives are very important in COBIT's world because it is the base of this framework on which it works and after that it has been organized into hierarchy of processes and domains that are basically for the alignment of business and IT objectives. Supporting IT, management all of them can use COBIT to help themselves provide a systematic control system for IT purpose. (Gail Ridley, 2004)

COBIT's model has to satisfy all the business requirements and the important information which are there has to meet these seven requirements which

are : 1) Compliance, 2) Efficiency, 3) Effectiveness, 4) Availability, 5) Reliability, 6) Integrity and 7) Confidentiality. The conceptual model which is being monitored will have to relate that each COBIT process has to go through some information criteria that the process affects, and therefore, it should provide an auditor that will process the whole scenario directly by assessing some of the specific controls for the quality of the information. COBIT information has on how have links with COSO's objectives that are related to the effectiveness and efficiency of the operations and compliance which will have all the laws and regulation to have the best reliable information. After all the process is through the main thing is to achieve the COBIT information criteria and all the important aspects for the information to be effective and efficient (Brad Tuttl, 2007). The audit process using COBIT 4.1 framework is shown in Figure 2.2 (Gusti Ayu, 2014).

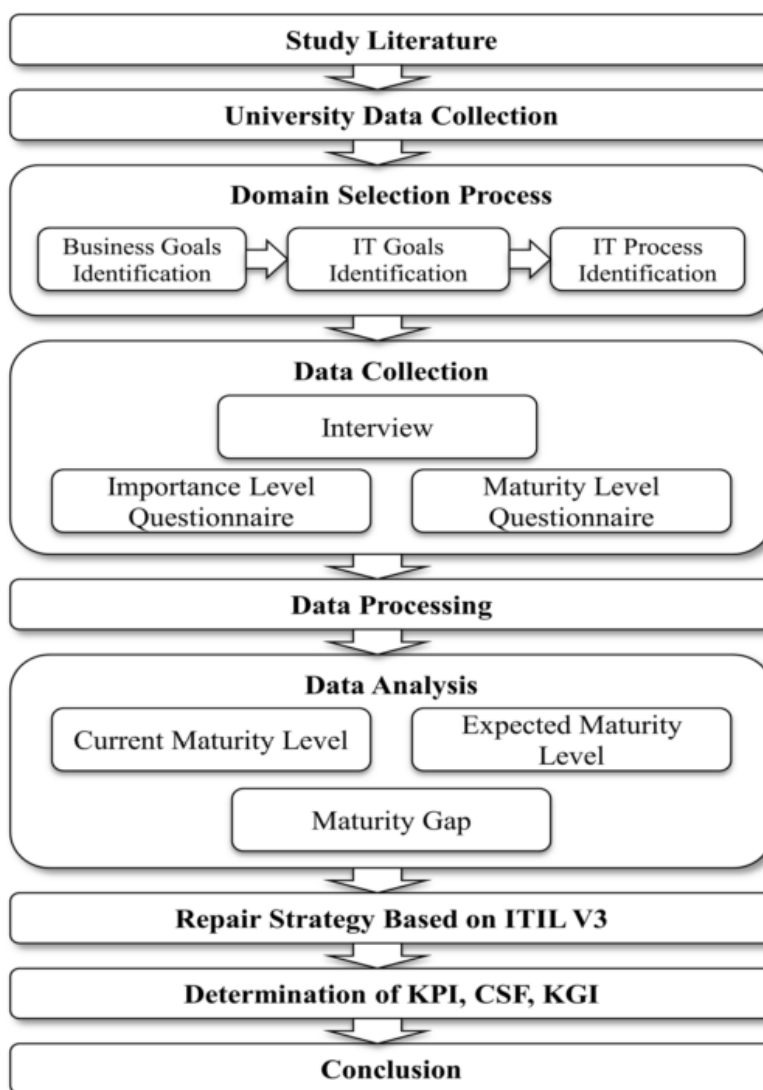


Figure 2.2 : Audit Process (Gusti Ayu, 2014)

2.3.2 COSO Framework

COSO was basically introduced as the first to have a well structured system for describing the internal controls and with that also the internal integrated framework which was in the year 1992 (Davis & Wheeler, 2010).

The entity of board members play an important role in internal control and the management and other personnel are to provide all the reasonable assurance to achieve these following objectives in order for Internal Control Process:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations.

The COSO cube for internal control-integrated framework (Davis & Wheeler, 2010).

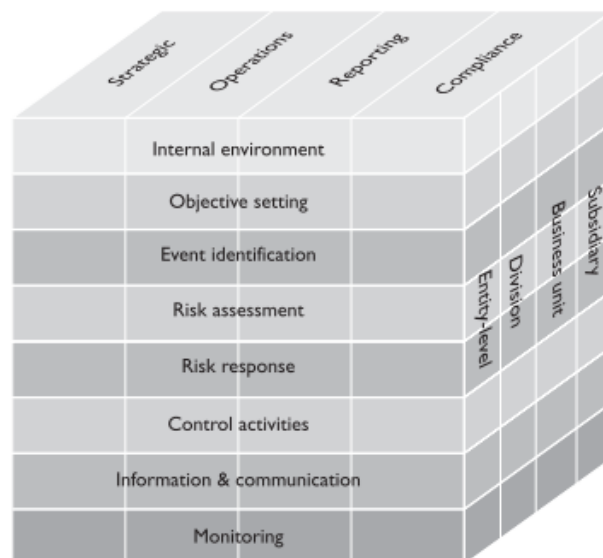


Figure 2.3: COSO expanded cube (Davis & Wheeler, 2010)

2.4 Database Security Audit Frameworks

Databases are usually one of the most important and compromised assets of any organization. Basically what hackers think is that databases are the heart of any organization which stores all the valuable and important trusted data. When the hackers get into the database system they can easily extract some important values which can cause loss and the operations can have an impact on the business as well at any time.

In addition to these economic losses or the status of the organization is damaged or breached can result into governing fines and a lot of fees would have to be paid for this. Thus, every organization needs to protect their valuable data as well as their databases. Database auditing involves monitoring and recording which can be made for only selected user database actions, so they can be aware what actions have the users got. Some of the security databases are shown below.

2.4.1 Integrity Framework for Database Audit

Databases nowadays are a very critical substance which every organization must protect for the sake of their private records. Integrity database log and audit framework is basically used of the Oracle Audit Vault and it can also be used for Database Firewall (AVDF). The Oracle AVDF is basically a simple tool which is mainly used for the database logging and auditing and the framework basically provides a methodology which if implemented can be applied to all the databases under Oracle AVDF (Michael A. Miller, 2016)

The framework has two basic benefits. First one is that it enables all the logging and auditing in the database source to provide alerts and reports in the context of AVDF. Secondly and the most important part also is that this framework will define the critical aspects that should be alerted and reported by using AVDF.

The installation of both the Oracle AVDF and the implementation of the framework will be completed in a few weeks, depending on the size of the number of source database. The most important factor is the amount of logging and auditing which are currently enabled in the database source.

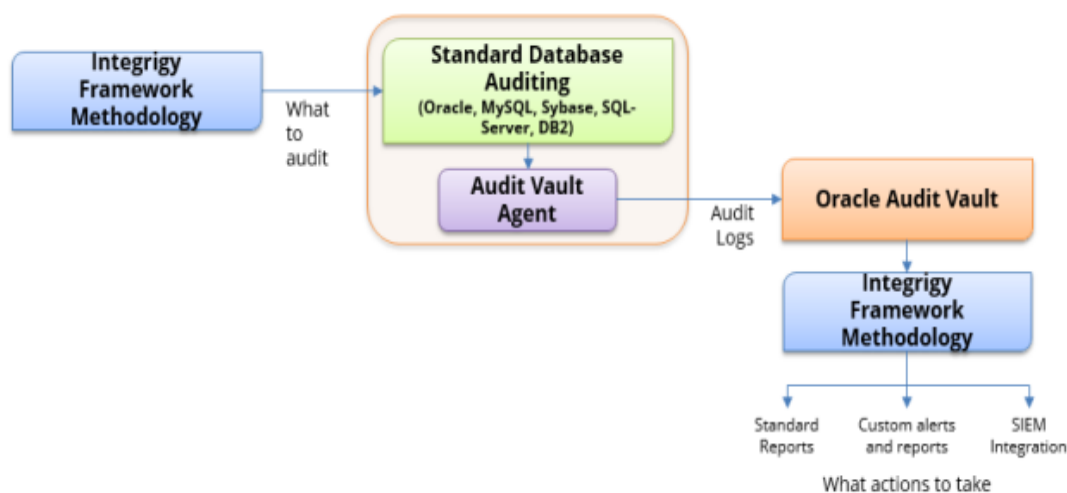


Figure 2.4: Integrity Framework Methodology for Database Audit (Micheal A.Miller, 2016)

2.4.1.1 Integrity Framework for auditing and logging of database

The direct result of the integrity consulting experience is by the help of the framework for database logging and auditing and it is also equally used for both who are starting to implement logging and auditing as well as those who want to enhance their capabilities. The main goal of this framework is the give a clear explanation of the auditing and logging features which are available, and it will also help to present

a deep approach for using these features which will lead to straight forward configuration approach as well.

The framework is helps specifically to design and help clients meet their compliance by some standards such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability ACT (HIPAA) and Federal Information Security Management Act (FISMA) (Micheal A.Miller, 2016). The foundation of the Framework is a set of fourteen (14) key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

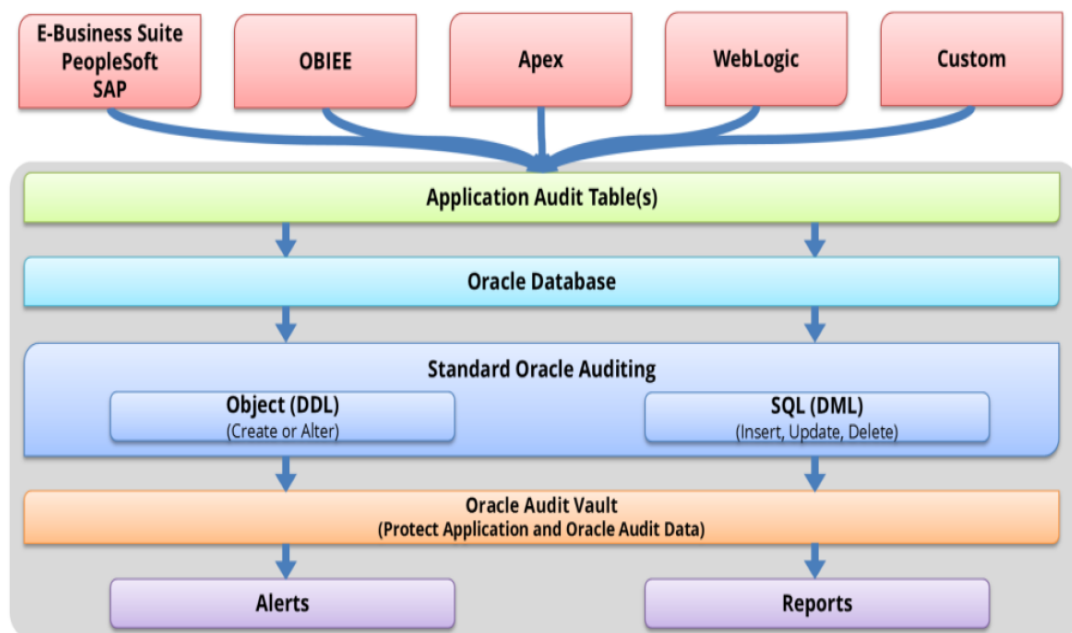


Figure 2.5: Integrity Framework for auditing and logging for database (Micheal A. Miller, 2016)

Table 2.1: 14 Key Security Events (Micheal A.Miller, 2016)

14 Key Security Events	
E1 - Login	E8 - Modify role
E2 - Logoff	E9 - Grant/revoke user privileges
E3 - Unsuccessful login	E10 - Grant/revoke role privileges
E4 - Modify auth mechanisms	E11 - Privileged commands
E5 - Create user account	E12 - Modify audit and logging
E6 - Modify user account	E13 - Create, Modify or Delete object
E7 - Create role	E14 - Modify configuration settings

2.4.2 Database Auditing for Oracle Database

Databases are usually one of the most important and compromised assets of any organization. Basically, what hackers think is that databases are the heart of any organization which stores all the valuable and important trusted data. When the hackers get into the database system they can easily extract some important values which can cause loss and the operations can have an impact on the business as well at any time.

In addition to these economic losses or the status of the organization is damaged or breached can result into governing fines and a lot of fees would have to be paid for this. Thus, every organization needs to protect their valuable data as well as their databases. Database auditing involves monitoring and recording which can be made for only selected user database actions, so they can be aware what actions have the users got. Some of the security databases are shown below (ElhamIskandarnia, 2013).

The auditing concept is basically for the prevention and the threats to be detected which will be provided in the framework in Chapter 4. Nowadays many of the organization are facing the same problems that is the security of their databases and are also realizing that how to recognize a threat and then treat that threat in a cost-effective manner. This audit concept will basically help the University-Based Organization to minimize the cost of the database security (Reena R. Chaudhari, 2015).

The conceptual framework for this is that the tools for the auditing is used by DBA and examines the locations where databases stores auditing records, and study the actions produced by Database Management System (DBMS) as well as add actions to satisfy the requirements. The Conceptual Framework is shown in the Figure 2.6 below.

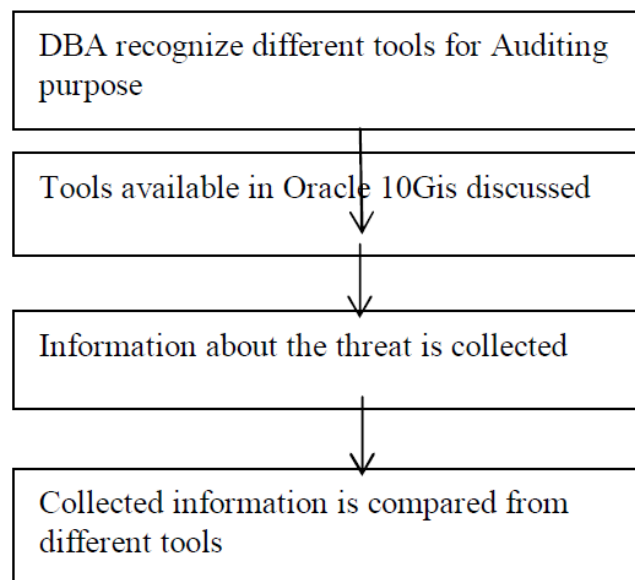


Figure 2.6: A Conceptual Framework (Reena R. Chaudhari, 2015)

2.5 Information security audit and assessment components

Figure 2.7 shows the main components of Information security audit and assessment



Figure 2.7: Auditing phases (Russel, 2013)

2.5.1 Preparation Phases

Everything that is conducted in advance by relates parties such as audit manager, auditor, and client to ensure that the auditing complies with clients requirements and objectives are during the audit preparation phases. In this first part of the audit process it usually starts with a reason to carrier out the audit. Auditor begin to analysis all the requirements and objective requested by clients. This phase consist of activities such as staffing the auditing group, and creating the audit project plan or blueprint before the actual implementation of audit (Russell, 2013).

2.5.2 Performance Phases

Russell, (2013) states that the performance phases of an audit is commonly defined as the fieldwork. Performance phase is the information collecting stages which covers the time period from arrival at the audit location until the exit meeting. Some of the on-site auditing activities includes meeting with the audit team member, communicate with team members and auditee, understand the fundamental of the process and system controls, analyse whether these controls work through verifying, and on-site information gathering such as firewall, server, network topology, router devices, existing policy, and other.

After that, laying down the groundwork for auditing member to conducts the audit process such as penetration test on organization parameters, reviewing or enhances the existing IT policy, analysis the strength of access control from both technical based and administrative based. The auditing process can be done either internally or externally. Lastly, analyse the audit results to prepare for the next phases of audit which is conclusion phases (Russell, 2013).

2.5.3 Conclusion Phases

The objective of the audit report is to address the outcomes of the audit investigation. The report ought to offer accurate and clean effective information as a useful management resource in addressing vital organizational problems. Activities execute on this phases are sharing audit results, writing audit results, and dealing with resistance to audit recommendations.

After that, an audit closure and follow-up will be carried on to further enhance or correct any mistakes during the auditing report. Lastly, as according to ISO Standard 19011, clause 6.6 states that “The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client.” And also clause 6.7 of ISO Standard 19011 continues by stating that verification of follow-up actions may be part of a subsequent audit as it is part of the building an ongoing audit programs. In the end, the audit procedure is considered cease when the document of report is issued by the lead auditor or after evaluation and follow-up actions are completed (Russell, 2013).

2.6 IT audit the analysis and impact of IT audit quality

Author Stoel et al (2012) had deliberated in detail that the audit quality of the IT and all of its importance with the IT audit. According to their studies, IT audits are basically done inside the organization to see the operations, effectiveness and the systems which are critical in terms of security so that they can identify and try to improve the areas which have weakness. The audit services are conducted or have the importance for doing these very special things to maintain the effect and sufficient manner.

IT audit has grown because of these two reasons: 1) the dependency on IT and the spending on it for business operation and 2) new laws are taken in which are all linked to the operations which are audited. IT audit in any organization has different objectives to achieve and it may also have multiple parties within an organization which because of it IT audit quality may have many different definitions. IT audit quality has a clear majority of things which are very important in the field of audit and assessment. These definitions may have many things such as effectiveness and completeness which are basically linked with the efficiency of the standards and most importantly the cost. One of the main concept of the audit of IT is to give

complete authority that the organization systems and process are meeting the objectives.

The responsibilities when there is an audit going on are huge and to be precise the focus is mainly on the information assets that are mostly controlled over by the management and the process that is running it. There are a lot of standards that are introduced or even built for this kind of purposes such as ISO, AICPA etc which also help in defining some IT audit quality. The organization which is being audit must take strict action and appropriate decisions regarding the scope, resources and the tasks and activities that have to be performed within the limits of the rules and regulation in the IT audit process. The IT objectives play an important role in auditing and organization so the management should first see that there should be specific resources which are to be given for a very reasonable reason for IT audit and by this it should enhance the quality of all the audit and as well as decrease the cost of the whole process. This also requires that the whole process should consider other attributes as well in order to get the right result. The performance and the outcome of this whole process might include availability of the auditee personnel which is a key point and the infrastructure on which this system is running or the organization behavior with the auditee which are auditing and the structure of the business which is being audit.

Due to the above, Stoel et al (2012) did a study on factors affecting IT audit quality in which factor analysis was performed unto a series of factors deriving from from multiple previous literatures. These factors were then evaluated in terms of their relative importance. The results are based on the factor analysis as well as the scores of these factors, 13 important factors which are very important for the IT Audit Quality were refined and perceived as the most important IT audit factors on IT audit quality, as shown in Table 2.2.

Table 2.2: Importance of IT audit factors on Audit Quality

Factor	IT Rank
Planning and methodology	1
Independence	2
Auditee Relationship	3
Auditability	4
IT and controls knowledge	5
Business process knowledge and experience	6
Responsiveness	7
Business environment	8
Auditor experience with auditee	9
Field work and audit procedures	10
Resource availability	11
Business scale and audit scope	12
Accounting knowledge and audit skills	13

Based on the above results, Stoel et al. (2012) in the discussion had further analyzed and interpreted why some factors were ranked higher or lower than the rest. Amongst the factors discussed were:

Planning and methodology was the highest rated factor due to the low standard approach that was made for IT audits. The variations of operating system platforms which have different areas of networks and the applications which are being used which makes organizations the method which will be used for the planning the audit process and after that performing also for the systems and the process is based on the technologies which are basically less reliable to be perceived which will be even more importance for the IT auditors.

Independence is a very important part of this process. The crucial part of this factor is IT audits are basically integrated sources which have a nature of IT that will have greater reliance on internal IT and business personnel to assist with all the data collections and as well as to analyze it. Similarly, the business process is a very good knowledge to have because it will basically go for the IT auditors and make them

understand how IT is supporting the business and that will be able to lower the IT issues.

Auditor experience with auditee is significant for basically the quality of the audit and may have been explained similarly to the difference which has two main things that are planning and methodology which are above everything i.e. because of the variability for operating systems and their networks and systems. Certainly, it makes a lot sense that with an experience auditee who is doing the audit will have more productive audits and due to his knowledge gained for some specific process or system.

IT and control skills define the area of expertise in which is important in the contribution toward IT audit quality.

Business scale and audit scope was found very limited in the previous studies done in the literatures and the prior literatures to the potential impact of the organizations assets which were being audited and by this the scale and variety of business activities are pure. The main interest is the role of IT to concentrate on the growth of business scale so therefore, with mergers and acquisitions of businesses, the potential impact on audit quality needs to be considered. The researchers believed this factor requires additional investigation and research.

2.7 Internal audit process quality

Havelka & Merhout (2013) had studied various prior literatures that pertain to the objectives of the audit process which are basically known as the effectiveness of the audit quality and as well as efficiency of the audit in which effectiveness and efficiency are also deemed as the key notions of quality- audit quality is basically a tool which is mainly used to measure the success for the audit process. Therefore, the above researchers in their study had recognized audit quality which is one of the most important outcomes of the audit process in which the quality of the audit was

included as the primary outcome in their proposed framework for the internal audit process for IT as shown in Figure 2.8.

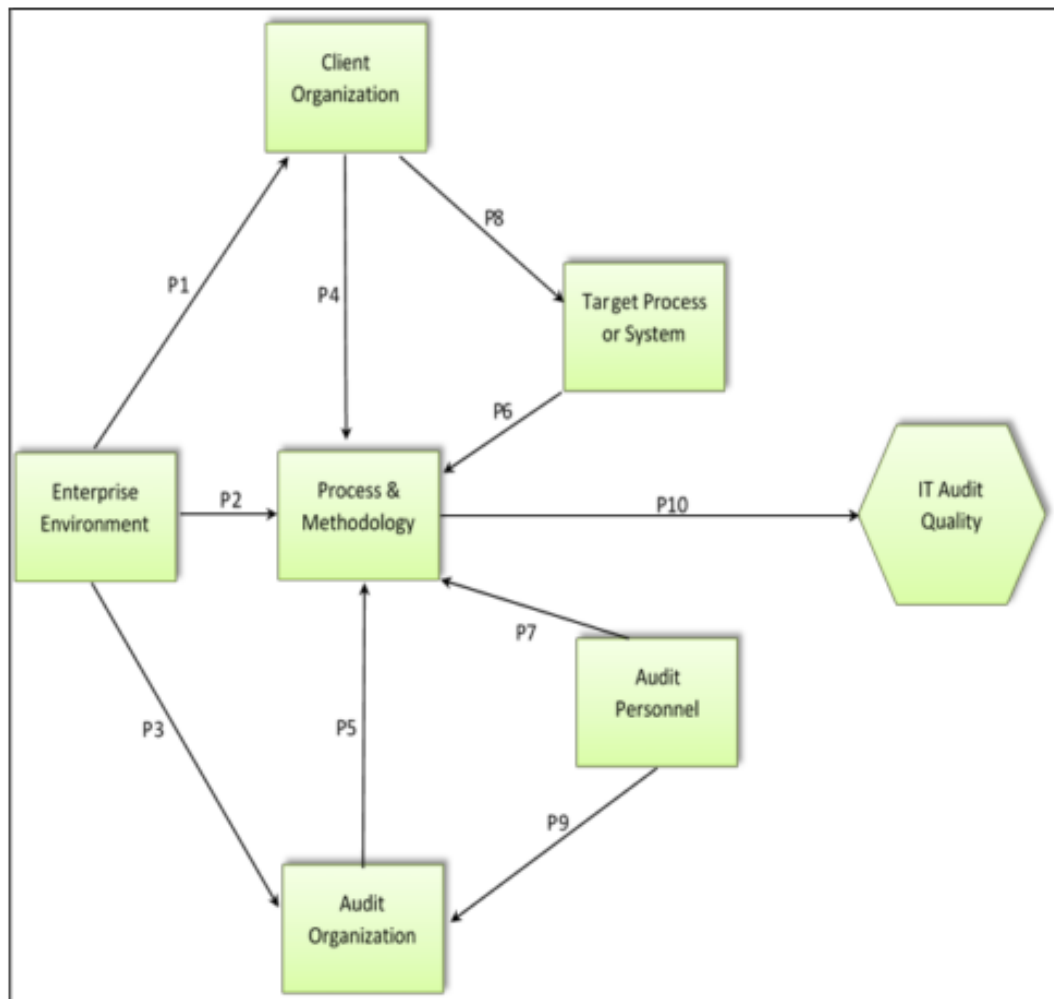


Figure 2.8: A theoretical framework for the IT internal audit process

Basically, the above framework as you can see has emerged with 26 different concepts with almost 6 categories in which it basically describes the codes and concepts which are presented. Summary of the Figure 2.8 details are presented through Table 2.3.

Table 2.3: Audit Process Quality: Categories, Concepts, Propositions and Indicators

Category	Concept	Propositions	Indicators
Audit Organization	Structure	P3: The Enterprise Environment will have a direct impact on the Audit Organization	<ul style="list-style-type: none"> • The audit organizational structure and reporting relationships to audit committee and auditees (independence) • Governance level issues (communication among IT audit staff)
	Operation	<p>P5: The Audit Organization will have a direct impact on the Process and Methodology</p> <p>P9: Audit Personnel has a direct impact on Audit Organization</p>	<ul style="list-style-type: none"> • Internal policies and procedures, external regulations, standards and best practices are followed • Management, support and direction of the internal audit team including vision, mission, and leadership of IT audit • IT audit staff management. Ability to attract and retain IT audit staff (recruitment, turnover of IT auditors) • Defined roles and responsibilities on the audit team and within the audit organization • Audit division feedback • Level of distractions (e.g. special projects, such as investigations that interfere) • Audit team reward structure must match enterprise (and client) objectives (e.g. # of findings vs. impact on openness of client)
	Resources		<ul style="list-style-type: none"> • Resources to create and document audit plan: databases, on-line forums (e.g. auditnet.org), tools, web sites, services • Resources available for the audit; staffing, tools, etc. • Resource availability, time and budget constraints • Computer-assisted auditing tools (CATs e.g. ACL) are available and used for testing and analysis • “Desktop” auditing – analytics
	Competence		<ul style="list-style-type: none"> • The level of experience of the IT audit staff • Maturity of IT audit organization
	Audit Team		<ul style="list-style-type: none"> • Audit team characteristics: team work ethic; character/integrity; willingness to learn; team cohesiveness/”get along”, team dynamics/synergy (individual’s personality) • Diversity of team (e.g. thoughts; ways of doing multiple measures; background; experiences) • Motivation of team, “sense of urgency”

Category	Concept	Propositions	Indicators
Client Organization	Audit posture	<p>P1: The Enterprise Environment will have a direct impact on the Client Organisation</p> <p>P4: The Client Organization will have a direct impact on the Process and Methodology</p> <p>P8: Client Organization will have a direct impact on Target System and Process</p>	<ul style="list-style-type: none"> • Client relationships, quality and responsiveness, honesty and openness • Support, cooperation, and buy-in exist from the client, auditee, and top-level (executive) management • Client understanding of audit process (and purpose of the audit) • Impact of audit rating/findings on auditee management's annual review or consequences to the business • Auditee's perception of auditor • IT organization/client morale • Client's mgt participation in definition of audit scope • Realistic expectation of audit • Environment of audit-physical location
	Structure		<ul style="list-style-type: none"> • The amount of organizational change, e.g. M&A, divisional restructuring, internal process change, and the organization's ability to manage the changes • Separation of management from operations-level employees of audited group, segregation of duties (SOD)/analyst not the code • One system platform (e.g., SAP) or "spaghetti" systems • Feedback mechanism from auditee/post-audit • Does business follow/embrace SDLC methodology? • SOX controls contained in the control framework
	Information (evidence) availability		<ul style="list-style-type: none"> • Complete, timely, and accurate data/info from client (e.g., via database or inquiry), documentation • Client understanding of business process (i.e. their own area) • Business unit utilization of self evaluation processes that mirror IT audit practice framework • Number of different recent audits (external and internal) in a particular area • Ability to gather independent data (rather than relying on client) • Business interruption (auditee not available/system down)
Enterprise Environment	Organizational communication	P1 (as explained above)	<ul style="list-style-type: none"> • Communication between auditor & auditees before and during fieldwork, diplomacy (tradeoff b/w forceful and good rapport)

Category	Concept	Propositions	Indicators
Enterprise Environment (cont'd)	and collaboration	P2: The Enterprise Environment will have a direct impact on the Process and Methodology of IT audit	<ul style="list-style-type: none"> Organizational communication Good relationship with technological staff (subject matter experts) across corporation
	Structure and culture	P3: The Enterprise Environment will have a direct impact on the Audit Organization	<ul style="list-style-type: none"> Integration of IT audit into the financial and operations (F&O) audit plan, coordination between F&O & IT auditors Negative stigma of word “audit”→“review” is more positive Healthy corporate culture Control environment (degree of control) Size of IT audit org in relation to size of company Clear distinction between audit and IT risk management Organization and departmental politics
	External considerations		<ul style="list-style-type: none"> Legal and regulatory guidelines and requirements Media attention
Process and Methodology	Planning	P2; P4; P5 (as explained above) P6: The Target Process or System will have a direct impact on the Process and Methodology	<ul style="list-style-type: none"> Audit methodology is used Review of prior audit work Long term audit plan and goals exist Planning, timing and duration of planning are adequate and comprehensive Timing of audit Appropriateness of the audit process and methodology to IT problems
	Project (audit) management	P7: Audit Personnel will have a direct impact on Process and Methodology P10: Process and Methodology will have a direct impact on Audit Quality.	<ul style="list-style-type: none"> Sufficient time is allocated to execute the audit (especially field work) Project management Flexibility (time) — able to change schedule when necessary Coordination with external auditors Defined checkpoints, toll gates, meetings (internally) to ensure that executives, lines of business, and audit teams agree on planning and fieldwork Ensure that new information affecting audit completion is evaluated in a timely manner by manager Timely oversight, feedback, and review; adequate supervision Review of fieldwork and reporting by a higher level person (ensure consistent reporting) Project objectives and scope are clearly defined and planned

Category	Concept	Propositions	Indicators
Process and Methodology (cont'd)	Audit impact		<ul style="list-style-type: none"> • Effective reporting mechanisms, distribution to client organization, audit committee, and finance; communicate project results to appropriate level • Follow-up on issues (close out observations, persistence, did auditee respond), a methodology for follow-up on observations is in place • Being able to see impact of work (of audit) • Ensuring timely issue of audit report • Advice to auditee that is specific and reasonable • Intent of audit (any hidden agendas or objectives)
	Audit practices and procedures		<ul style="list-style-type: none"> • Documentation (work product) standards, results are documented to appropriate level of detail (as evidence to support findings, to be able to re-perform work, for efficiency, over-doc) • Documentation templates and forms exist and are used • Adequate testing is performed and meets objectives, tests assertions, and supports conclusions • Well-written conclusions based on tests performed, adequate support for conclusions exist • Representative sampling is used Identify control gaps and assigning ownership to remediate • Control identification (Preventative, Detective, Corrective categorization) • Proper use of facilitation and collaboration techniques • Willingness to admit weakness or gaps in audit plans • Conflict management
	Risk orientation		<ul style="list-style-type: none"> • Risk assessment process — use of continuous process • Risk-based audit approach is used, the risk assessment model is understandable to auditee and audit team
	Quality assurance		<ul style="list-style-type: none"> • Quality assurance process (internal) — audit the auditors • Metrics to measure quality exist (metrics vs. standards) • Design of quality test steps

Category	Concept	Propositions	Indicators
Target Process of System	Characteristics	P6 (as explained above) P8: Client Organization will have a direct impact on Target System and Process	<ul style="list-style-type: none"> • The complexity, type (in-house v COTS), and size (volume) of the application, system, transactions, or unit being audited and the IT environment • Accuracy and reliability of data in system • Overall risk rating of area being audited • Routine audit vs. non-routine special project • Manual vs. automated process under audit (level of automation in business process) • Primary intention and use of system by auditees every day, purpose of the system
	Design		<ul style="list-style-type: none"> • Existence and effectiveness of key controls and their effect on testing • Auditability of system being audited • Well defined organizational standards and processes (of auditee) and adequate documentation of these • Availability of documentation • System flow charts
Audit Personnel	Communication and collaboration skills	P7; P9 (as explained above)	<ul style="list-style-type: none"> • Interpersonal skills of auditors, including written and oral communications skills • Effectively work in a team environment (business & technical audit together integrated audit) • Report writing/documentation skills
	Domain and process knowledge		<ul style="list-style-type: none"> • Knowledge of business of auditee (industry, organization, and business unit) • Auditor understanding of supported business processes • Understand business rules (does code match), subject matter
	Career development		<ul style="list-style-type: none"> • Effective work/life balance and job satisfaction • Training and development Professional certifications
	Professional skills		<ul style="list-style-type: none"> • Time management Auditor objectivity • Ability to concentrate on facts (by auditor & auditee) — keep emotions in check • Conflict resolution and negotiation skills • Auditors & auditees ability to work through “challenging” environment • Ability to multi-task on multiple projects and be able to prioritize • Auditor decision making skills • Ability to build consensus or solutions

Category	Concept	Propositions	Indicators
Audit Personnel (cont'd)	Personality traits		<ul style="list-style-type: none"> • Competence of the IT auditor and client personnel • Positive attitude of auditor • Ability and willingness to continually learn • Willingness and ability to change (individual level)
	Technical skills and knowledge		<ul style="list-style-type: none"> • Level of technical expertise • Understand why technology is being used and the associated risks • System code understanding • Knowledge of technology infrastructure within the organization, knowledge of systems integration
	Audit skills and knowledge		<ul style="list-style-type: none"> • Auditor judgment (e.g., assessment of risk rating) • Ability to map processes and data flows through systems and identify central points • Understand output of testing results • Ability to identify control weaknesses • Financial audit knowledge • Knowledge and ability to use audit tools

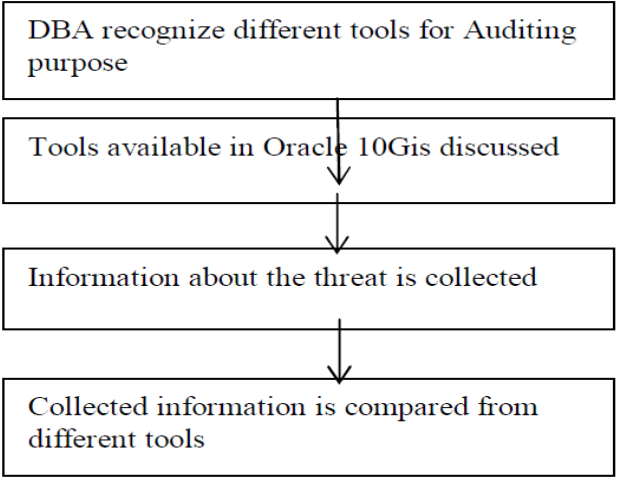
The framework was derived from a multitude of prior literatures that support the concepts in the proposed framework i.e. concepts were based on gaps found in prior research in which some categories or concepts could either be not relevant or significantly influential and that most literatures which are generally focused just on audit and the internal audit whereas the basic a research will be focusing on auditing which was inadequate. As a conclusion, the research had identified the following implications for future research such as: 1) Accurate validation and testing of the proposed framework; 2) extensive studies were done to determine the nature for each concept so that to develop its relationship to audit outcomes; 3) statistical models were combined and used through quantitative methods in order to effect the audit quality; 4) further develop the proposed framework by using qualitative or a survey method e.g. a case study, questionnaires or interviews; the research was made more additional in order for the audit process quality to see both the effectiveness and efficiency of the audit (Havelka and Merhout, 2013).

2.8 Previous Frameworks Comparisons on Database Audit

The following table 2.4 illustrates the previous frameworks strengths and limitations on database audit.

Table 2.4: Comparison of previous frameworks on database audit

Framework/Authors	Diagram	Components	Strength	Limitations
<p>Integrity framework for database audit (Michael A.Miller, 2016)</p>		<p>Standard Database Auditing, Oracle, SQL, Oracle Audit Vault, Reports, Alerts and Object(DDL).</p>	<p>Framework tries to understand the concept of database audit by using of database audit vault. This paper describes how to do the audit by logging and monitoring the database.</p>	<p>The framework is not comprehensive to be widely used, the framework did not mention about in details that how to replicate or copy the application log and audit data.</p>
<p>Integrity framework for auditing and monitoring of database (Michael A.Miller, 2016)</p>		<p>Standard Database Auditing, Object(DDL), SQL(DML), Oracle Audit Vault, Alerts and reports</p>	<p>The framework discussed is to explain how individuals participate in database to foster relationships, the paper introduced a positive path for auditing and monitoring of the database. The Audit vault will be an integral part of</p>	<p>The framework did not discuss in detail the tendency towards the increase in alerts and reports of the audit system, the paper did not put much details in the primary benefit of the auditing and monitoring which is very crucial to know.</p>

			<p>the process to provide efficiency in audit.</p>	
<p>Database auditing for oracle database (Reena R. Chaudhari, 2015)</p>	 <pre> graph TD A[DBA recognize different tools for Auditing purpose] --> B[Tools available in Oracle 10Gis discussed] B --> C[Information about the threat is collected] C --> D[Collected information is compared from different tools] </pre>	<p>Oracle database controls, tools for auditing, alerts, reports, information about the threat, access control, object</p>	<p>The framework described how to keep safe and secure the information in an oracle database system. This framework provides the large amount of security to the database, this paper will unsure that the DBA of database management system needs to secure a particular database system.</p>	<p>The framework components are limited. The framework did not focus on how to educate the users of the request was modified, then what data was changed, the paper does not tell us that who access the data and what time and date was the access. The paper also doesn't tell that what program or client software was used to access the data</p>

<p>Internal Audit process quality Havelka & Merhout (2013)</p>	<pre> graph TD EE[Enterprise Environment] -- P1 --> CO[Client Organization] EE -- P2 --> PM[Process & Methodology] EE -- P3 --> AO[Audit Organization] CO -- P4 --> PM CO -- P8 --> TPS[Target Process or System] AO -- P5 --> PM AO -- P9 --> AP[Audit Personnel] AP -- P7 --> PM AP -- P6 --> TPS TPS -- P10 --> ITAQ{{IT Audit Quality}} </pre>	<p>IT audit quality, audit organization, enterprise environment, audit personnel and client organization</p>	<p>This framework offers users a platform to build and maintain the effectiveness of the audit quality as well as efficiency of the audit.</p>	<p>Framework doesn't specify the main important steps which takes us to the audit rather then just making the quality of the audit more better. The audit process was not explained at all.</p>
<p>Database Autopsy Close Look to Database Auditing for Oracle Database (ElhamIskandarnia, 2013)</p>	<pre> graph TD A[Identify different tools DBA can use for Auditing purpose] --> B[Discuss available tools in Oracle 11G with grade] B --> C[Analyze the tools and extract information about the threat] C --> D[Compare extracted information from different tools] </pre>	<p>Oracle database controls, tools for auditing alerts, reports, information about the threat, object, access control</p>	<p>This paper provides an important role of auditing not only detecting mistrustful behavior but also providing proof and reasons to auditors that it is recommended to used oracle database auditing because of its minimal impact.</p>	<p>This framework is not fully implemented on oracle databases. The framework did not mention about the privacy and security concerns in details.</p>

The justification of the selected components is based on the authors. Thus, most of the authors discussed the common components which are very crucial for this project research. As there were common components which have been repeated by most of the authors are been selected to be applied and adapted in the research project. The researcher has chosen those components because of their significance and good to be adapted in this research project. Another hand, in term of the limitations of those frameworks, the authors did not fully cover the importance of audit quality in details. The previous frameworks did not mention fully the use of audit quality and access control in details because of that, the researcher has selected those components to expand more details of the quality of the audit in the database audit. In addition, in term of features selection, the researcher wants to adopt those components in this research project to provide a huge contribution in order to make the audit experience better. Previous frameworks limitations have been discovered such as Lack of audit quality that discusses how we can improve the standard of auditing in database. There was a limitation from previous framework which doesn't specify how to replicate the application log and audit the data.

Moreover, the researcher chosen Oracle database controls as a component to adopt in this research project is to educate the users to know about how the controls takes place when auditing an Oracle database. Besides, the researcher chosen Object(DDL) and SQL(DML) as components is to keep confidential and personal information of the database to be secured and the researcher has chosen Access Control to have the database physical security as well as database logical access to make the audit more efficient. As a summary the researcher chosen those components to adopt in this research project since, many authors discussed the same components which has been listed below.

Therefore, the selection of those components can be good example to adopt in this research project. The selected components will comprise of the below named components which includes the following:

- i. Access Control
- ii. IT Audit Quality
4. SQL (DML)
5. Object (DDL)
6. Oracle Database Controls

2.9 IT Information Assets

Information Assets are important in field of IT. By understanding that what is the information that is being given and how to protect it, this becomes very vital and it should be understand at the very beginning that it will mean by the word information asset. Information asset can be defined as the information that can be managed as a single unit which can be exploited, protected and can be understood. That is why the assets are the most important part of any organization database and because of the sensitive information they possess that's why these assets or information needs to be secured (Archives, 2017).

The basic concept here is make manageable portions by making groups of your individual pieces of information. if you had to assess a huge amount of document, database and pieces of record you hold then you will have an impossible task by having a list of millions of items. If we make grouping the items at a level that will match your objectives then you can make the task equal to achievable (Archives, 2017).

The information assets are very important hence it should be identified according to the information that has been given above and to consider the extent of great ease that is required to achieve the goals. There are so many different stages

where the information asset can be defined that will allow its constituent components to be managed as a single unit (Rouse, 2013).

It is probably the simplest to start with a very massive definition after then breaking the information to a very reasonable grouping up till appropriate size. To determine that whether something is an information asset or not, it can be identified by the following questions in figure 2.6.

Table 2.5: Table of question of define assets (Institute, 2016)

<p>Its Value</p>	<ul style="list-style-type: none"> • Does it have a value to the organization? • Will it cost money to get this information again? • Would there be legal, reputational or financial repercussions if you couldn't produce the information on request? • Would it have an effect on operational efficiency if you could not access the information easily? • Would there be consequences of not having this information?
<p>Risks</p>	<ul style="list-style-type: none"> • Is there a risk associated with the information? • Is there a risk of losing the information?

	<ul style="list-style-type: none"> • A risk that the information is not accurate? • A risk that someone may try to tamper with it? • A risk that arising from inappropriate disclosure?
Content	<ul style="list-style-type: none"> • Does the group of information have a specific content? • Do you understand what it is and what it is for? • Does it include all the context associated with the information?
How you manage it	<ul style="list-style-type: none"> • Does the information have a manageable lifecycle? • Were all the components created for a common purpose? • Will they be disposed of in the same way and according to the same rules?

1. Does the information have a value to the organisation?
2. How much cost or money to reacquire the information?
3. Reputational, legal, or financial repercussions if the information cannot be produce on request?
4. Would operational efficiency being compromise if users could not access to the information?
5. What are the consequences of not having such information?

6. Is the information associated with risk?
7. Is the information containing valuable values to organization?
8. Is the information valuable to other that might try to tamper it?

By answering the question above, it is believed that organization will be able to determine their own information assets within their organizations.

Examples: Information asset
A database of contacts is a clear example of a single information asset. Each entry in the database does not need to be treated individually; the collection of pieces of data can therefore be considered one information asset. All the pieces of information within the asset will have similar risks associated with privacy and storage of personal information.
All files associated with a specific project may be considered a single information asset. This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All the individual items can be gathered together and treated the same as they have similar definable content, and the same value, business risk and lifecycle.
Depending on the size of your organisation, you may be able to treat all the content in your electronic document and records management system as a single asset – but this could be a risk as such a large asset containing varied types of content is likely to be hard to manage.
All the financial data for an organisation could be considered a single asset. There are very specific risks to the business if this information is mismanaged and you may also have an obligation to provide transparency of information, which could be problematic.

Figure 2.9: Example of information assets (Archives, 2017)

2.10 University-Based Organization

2.10.1 UTM (CICT)

Universti Teknologi Malaysia is an innovation-led University. It has two campus. One is located in Kuala Lumpur which is the capital of Malaysia and the main campus is located in Johor Bahru which is southern city in Iskandar Malaysia, which is a hub of economic corridor in the south of Peninsular Malaysia.

Center for Information and Communication Technology (CICT) is the main branch in UTM that has all the available Database of the whole UTM. It has many important things such as ID accounts and access of all the staff and students with email, ICT security, High Performance computing, UTM storage and Video Conferencing and Streaming. All of these things need to have a backup plan so that the data which is required from these areas does not get affected or lost by any malware attack. So, auditing this whole CICT database system will improve many things such as Firewall policy, URL filtering, Application control and intruder prevention system. ICT security in CICT holds very important role because it is used to provide and manage next generation firewall with reducing complexity and lowering the total cost of ownership. Implementation of high availability concept with active-active balancing will be to optimize the functionality and efficiency.

2.11 Summary

This chapter basically is describing all the important variables and previous frameworks about information security database audit and assessment. Information assets and the audit procedure are also given in this chapter to provide valuable information regarding auditing. This chapter's purpose is to provide the details of the audit process and to fulfill the requirement of getting the important variables for the initial framework for this thesis that will be discussed in chapter.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter reviews the literature about information security database audit and its assessment and how there is a problem in the audit quality of databases in organizations. The researcher reviewed the concept of how the database audit take place in information security platform and the concept of some conceptual frameworks for the betterment of the audit when it takes place. This concept if of qualitative nature and tends to improve the quality of audit and its assessment in databases.

Project methodology is the way to provide the researcher a way to carry out the research and experiments towards the problem gap. The study of this research will help in making a better Audit quality for the database to improve the information security decision making in areas like Audit, Assessment and Risk Management. The developed Information Security Framework will improve the security of private information in databases and it will help on technical bases as well. By auditing of databases, it will be the key to secure the university Assets and information systems for the betterment of the related university in coming years.

The enhancement of this framework forms the comparison of COBIT and COSO will affect the security level of the information systems and its databases that are in the University and it will make a Risk-free environment in all parts of the faculty. This framework will also show the detailed structure of how to apply auditing and monitoring of database by using some policies regarding this matter. Information security audit in this research will help in understanding how to review security permissions through registry editor and how to manage different types of account that are available on that database. By this IS auditor will have a chance to audit the databases with more accuracy and importance.

The research methodology covers activities and operations that will be carried throughout the implementation of this research project. The project is divided into these three 3 major phases which are shown in the Figure 3.1 and the summary of the phases used in this research methodology are given in Table 3.1.

3.2 Research Operational Framework

Operational frameworks are basically described as the systematic view of some operations which are involved which will make this project an immediate success. The operational framework describes the methodology step by step and also it provides some procedures so that the project can be explained and conducted in a suitable way. The operational framework shows all the correct methods which are used to complete this research with more clarification and the connection between various variables are also under supervision with the help of this framework. The research operational framework gives the in depth understanding of the process to achieve the research objectives of the research project. The overall process of the project is divided into phases and sub-phases. The project contains three objectives and to fulfill the objectives the research project has three major phases. Below figure 3.1 shows the visual representation of the research framework.

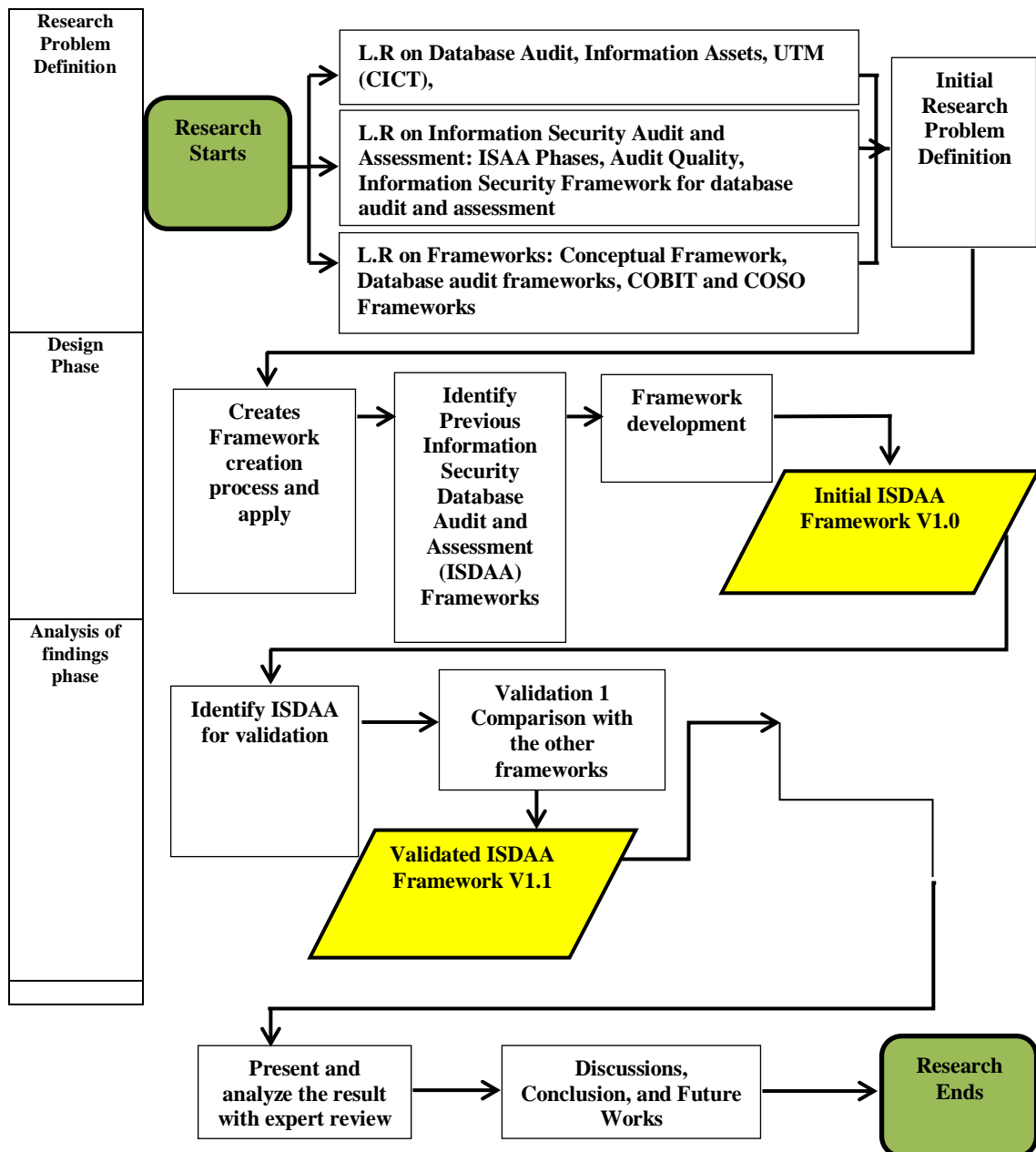


Figure 3.1 : Operational Framework

Table 3.1: Summary Phase of Research Methodology

Phases	Activities	Deliverables/Output
Phase I: Research Problem Definition	<ul style="list-style-type: none"> • Project Domain Identification • Determine the research field • Plan the project • Find out the problem and issues • Define project aim and objectives • Define scope of the project • Gather the project requirements • Determine problem statement • Database Audit 	<ul style="list-style-type: none"> • Submission of the proposal • Identify the problem of study • Define project aim and objectives • Define scope of the project • Identify significant of the project • Define database audit • Study the features of database audit • Identify the cause of the problem
Phase II: Design	<ul style="list-style-type: none"> • Previous Conceptual ISDAA Framework • Data Collection • Primary Data and Secondary Data collection • Design of conceptual Framework 	<ul style="list-style-type: none"> • Initial Framework from the previous frameworks • Gathering of required data • Analyze data properly and address related work
Phase III: Analysis and Findings	<ul style="list-style-type: none"> • Comparison Validation • Previous frameworks will be compared • ISDAA initial framework 	<ul style="list-style-type: none"> • Expert Review • Comparison validation done

3.3 Project Phases

3.3.1 Phase 1: Research Problem Definition

In the first phase the planning of the project takes place. It starts with the identifying of the objectives, aim, problem background as well as the problem statement faced currently by database audit. Firstly, the aim which is to design a conceptual security framework for database audit and assessment in a university and then the objectives of this project which is to study the audit quality of the database in the university organization. A proposal form was filled which include the background of the study, problem statement and an objective. The objective of the study was derived from the problem statement.

The focus of this project is on the information security database audit and its assessment and how we can improve the audit quality by developing a conceptual framework. Stoel et al. (2012) had explained in detail the importance of IT audit and audit quality. According to the studies the IT audit is widely used by organization internally to examine the operations, effectiveness, controls and security of critical systems to identify opportunities for improvement or areas of weakness. The increased demand of the IT audit services makes the importance of formulating these services in the most efficient and effective manner. In this case there are specific standards that will be used to assist in defining certain IT audit quality E.g ISO.

In this phase the effective reporting mechanism, distribution to client organization, audit committee and finance will communicate project results to the appropriate level in order to improve the audit quality. The quality steps will be designed in this phase as well as the use of quality assurance process which is also called internal audit will take place as a survey to have quality assurance in this audit.

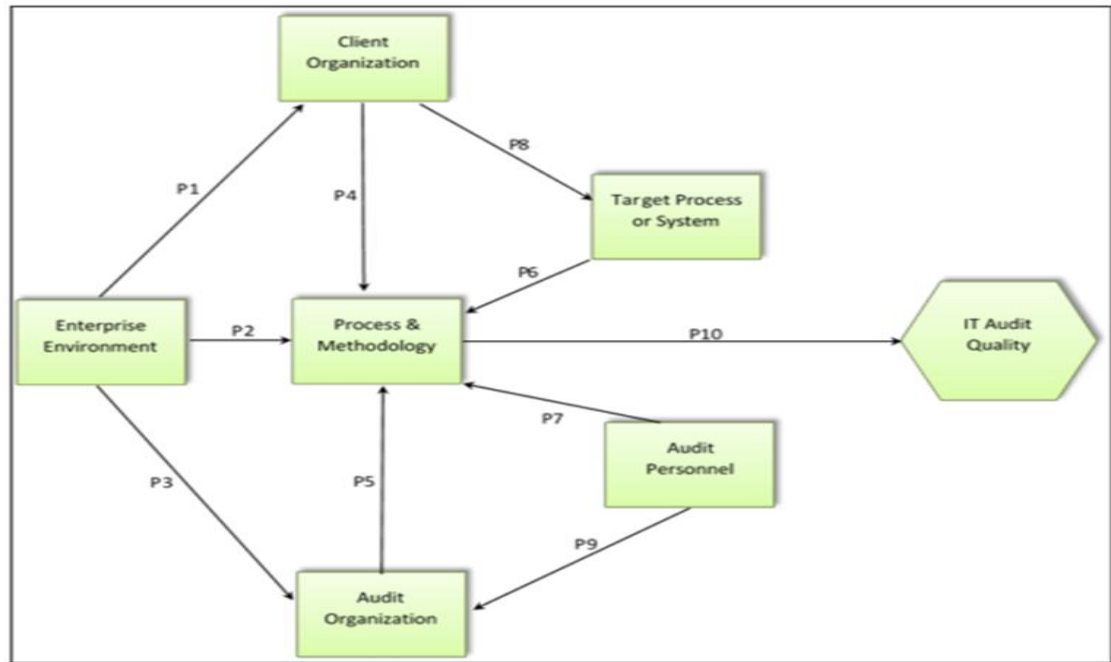


Figure 3.2: A theoretical framework for internal audit process

The audit quality will work exactly near to the process which shown in the above Figure 3.2. The P's which are shown in the above Figure are the 10 process from which this internal audit process has to go thorough to get the IT Audit quality.

3.3.2 Phase 2: Design Process

The design phase consists of the development of a conceptual framework which will be driven by the rigorous study about the existing methods for security audit on database. Basically the audit process of the audit process will be described with the help of this researched conceptual framework by doing a thorough survey of the place where the audit will take place and the questionnaire will also help us in making the framework more precise and accurate.

The conceptual framework will have different paths that will make sure that the reader gets the full knowledge of some things in the audit which are :-

- i. The audit takes place because of a certain reason.
- ii. Review of prior audit work.
- iii. Long term audit plan and goals exist.
- iv. Planning, timing and duration of planning are adequate and comprehensive.

The design of this framework will be by substantial validation and testing by the proposed framework and it needs extensive studies for each concept identified to determine the nature of its relationship to audit the outcomes and to further develop the framework via a survey or qualitatively e.g. interviews, and/or case study and the research about the audit quality for both effectiveness and efficiency of audit will take place for this framework to be completed and used in the future. This framework will also show the detailed structure of how to apply auditing and monitoring of database by using some policies regarding this matter.

3.3.2.1 Data collection

The collection of data has nowadays become very important in any research field. It basically gives all the valuable information for achieving results of the basic research. The methods which are used in collecting data for this study have both types of data which are primary and secondary data. Data collection is basically a simple procedure which most of the researchers follow to collect and gather data and information from the respondents. Data collection is precisely the study which is divided into two main subparts which are primary data collection and secondary data collection.

i. Primary data collection

The data's primary source in this collection is the questionnaire. The data was collected through the use of questionnaire from the UTM (CICT) staff and do the face to face interview with the database manager of the database system area. The questionnaires are designed to get fast reaction and data from the targeted respondents on a wide range for database audit quality concern. The questions will be mostly closed ended questions and there are some open-ended questions as well. This type of data collection is that you must conduct your own data collection in order to gather or extract some information regarding the topic from the targeted users. This research basically chooses primary data collection which is to be carried out in a very reliable method for primary data collection only for this study.

ii. Secondary data collection

The secondary data collection can be found by using or focusing on the literature review as well as in the introduction as well. The secondary data is gathered mostly by books, journals, electronic resources and other related projects as well. Secondary data is very important in terms of providing the base from the literature study and it helps the researcher as well with a broad view about the knowledge of the topic of research. Every study must be started by secondary data so that much important it is for the research purpose. Secondary data collection is generally for discovering some study which include some information from the background or from the problem statement as well and in the discussion part which is included in the conclusion of the study.

3.3.3 Phase 3: Analysis of Findings Phase

This is the analysis of findings phase where data will be analyzed and aim of highlighting useful data .will evaluate the proposed strategy and provide their feed backs. This will be retrieved by the research and evaluated. The procedure of coordinating data is the key to understanding what the data does and does not contain. There is collection of method in which people can easily manipulate data across the analysis phase to push certain conclusion or agendas. For this reason, it is vital to pay attention after the data analysis is presented and to think critically concerning the data and the conclusion that drives. In addition, evaluation is a method used to test the design of the system to ensure that it meets the expected purpose and meet the user requirements.

Security audit checklist has a very important part to play in the audit and it helps the audit go smother and faster and there will be less mistakes in the audit because if you do a process which is in the list and after finishing that process you make in the checklist as done then in the end of the audit when you will be evaluating and checking all of the things for the last time then this checklist will help you in getting the right result.

3.4 Summary

This chapter serves the purpose for the details of the processes which are carried out to complete and fulfill the research objectives for this research project regarding information security database audit and assessment. This chapter shows that the processes are distributed into 3 main phases which in detail describes how this project will work and the details of this phases are given in a systematic way. The research framework will determine how the process will work in this project.

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 Introduction

This chapter will discuss the design of the research. The proposed framework components will be the focus of this chapter which summarized in the previous chapter. This chapter will clarify the main objectives of this research which is to identify the audit quality based on database audit and assessment through a conceptual information security framework. Most importantly this chapter will show the design of the questionnaire that will be distributed among the staff and students as well as the Audit checklist will be made for database. The initial proposed framework will be designed in this chapter in order to improve the audit quality through survey by questionnaire.

4.2 Initial Proposed Conceptual Framework

The proposed framework is based on the previous studies that have been discussed in the literature review. Auditing of Database must be done on a periodic basis. There are three main reasons to this. Firstly, periodical assessment can mitigate the risks introduced by the database system. Secondly, efficiency of controls relating to the database can be evaluated and finally, the audit review can help to continually

improve internal process, procedures and tools thus the overall effectiveness and efficiency of database system(s) implemented.

Having said the above, there was no dependent variable defined for this study because participants were required to focus more on the audit processes that influence security audit quality. Therefore, the security audit quality was qualified as the evident outcome of the proposed model as shown in Figure 4.1. The audit quality signifies the construct to measure the success of the database security audit process by assuming that each factor that contributes to the quality have a direct relationship with it.

IT audit quality as a construct and the key concepts of quality (efficiency and effectiveness) have been validated by several previous studies which were discussed in Chapter 2 of this report which amongst others are Havelka & Merhout (2013), Stoel et al., (2012), Rainer, (n.d.). Based on these studies, the effectiveness and efficiency and the overall quality of an audit requires gathering of competence evidence and auditors must understand a specific subject matter well enough to plan and perform efficient and effective audit.

In other words, an audit effectiveness/efficiency is the main objective of an audit process thus in this study, the database security audit quality is determined as the primary end result (component) of the conceptual model. Figure 4.1 shows the proposed conceptual framework version 1.0 (V1.0) which is derived from the previous studies as mentioned in Chapter 2. The Version 1.0 is taken from the proposed framework form Chapter 3.

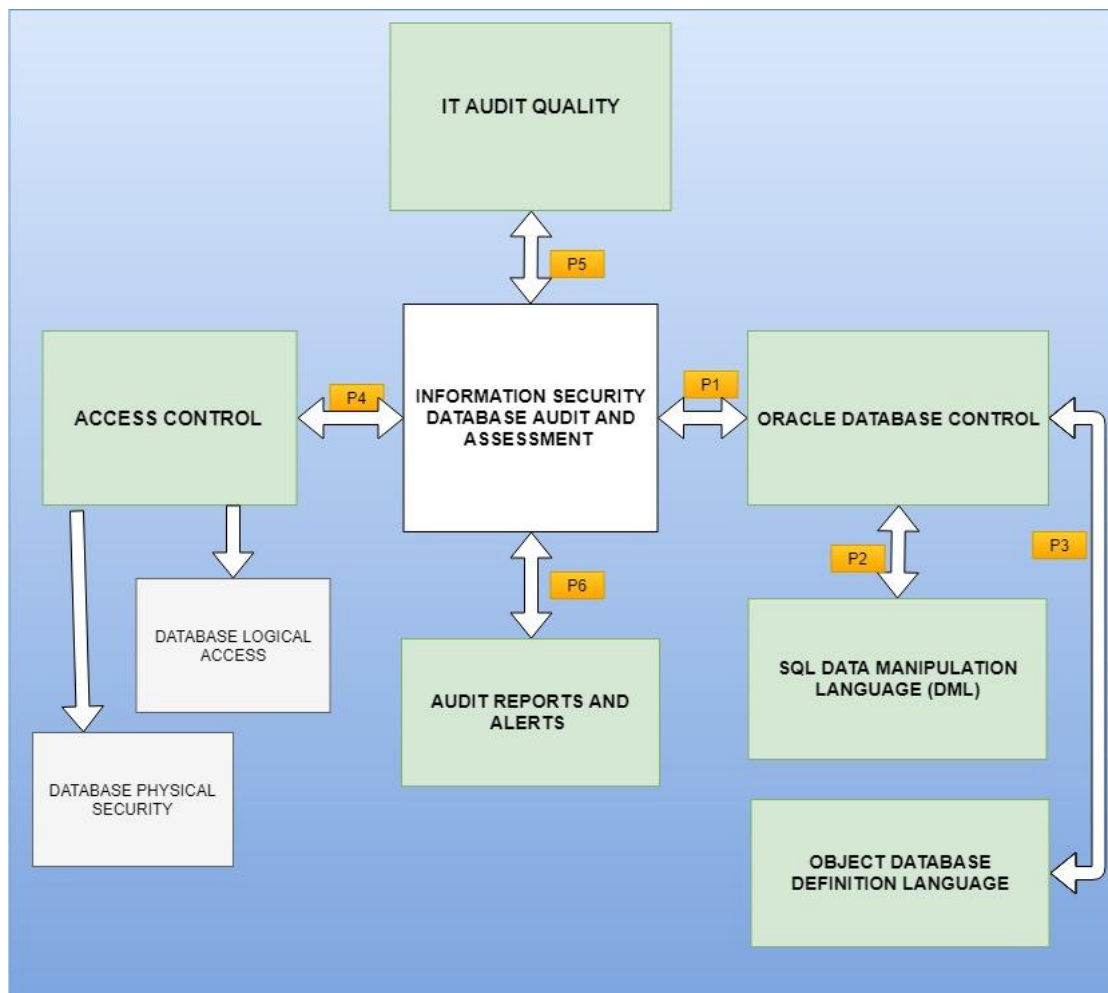


Figure 4.1: Initial Proposed Conceptual Database Security Framework

4.3 Oracle Database Controls

The P1 is the audit process which will take place will be the database controls. A database is basically a collection of all the related data which is organized in such a manner that it can be accessed by multiple users for valid purposes. Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment and manages some large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivering is in high performance.

Oracle database system was designed as the first database for different enterprises so that the cost-effective way should be flexible enough to manage different information and applications. Enterprise grid is basically an architecture in which each new unit is rapidly provisioned form the components. For the capacity to be added or relocated from the resource components there will be no need of workloads.

The database has basically two types of structures: a) Logical Structures, b) Physical Structures. Because both the structures are different and separate, the physical storage of data can be managed without interfering with the logical storage patterns.

The oracle database will be the focused database to audit in CICT, UTM. There are 2 kinds of databases in CICT:

1. Oracle Database
2. SQL Database

4.3.1 Object (DDL)

The P2 of the audit will be Object DDL. A data definition language or data description language (DDL) is syntax similar to a computer programming language for defining data structures, especially database_schemas. In the auditing phase of the database this command comes under the standard oracle auditing and is basically to create and alter the objects.

The access and usage of some objects can be audited by allowing object auditing. The statement/privilege auditing is a very important part of this process which can be limited enough to audit some specific users. Object auditing has many users but it has only a limited of one object to be audited. The AUDIT ANY privilege is required to have an object audit which should be general in all aspects. However, only the object owner can determine whether to enable or disable auditing on some owned objects as well as see some audit options for currently enable object. (Reena R. Chaudhari, 2015).

4.3.2 SQL (DML)

The P3 of the audit process that will take place will be the SQL DML. DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: *SELECT*, *UPDATE*, *INSERT* statements. In this the statements which are given above will be created once the audit of the database is done. Oracle supports three different kinds of audits enabled via various syntax of the SQL command Audit:

1. Statement
2. Privilege
3. Object

Oracle database standard auditing can be defined for the following –

1. **SQL statements** – Data Manipulation Language (DML) statements such as when users are attempting to query the database or modify data, using SELECT, INSERT, UPDATE, or DELETE.
2. **Database Schema Objects** – Data Definition Language (DDL) statements when users create or modify database structures such as tables or views.
3. **Database Privileges** – Audit can be defined for the granting of system privileges, such as SELECT ANY TABLE. With this kind of auditing, Oracle Audit Vault records SQL statements that require the audited privilege to succeed.
4. **Fine-grained audit conditions** – Fine Grained Auditing activities stored in SYS.FGA_LOG\$ such as whether an IP address from outside the corporate network is being used or if specific table columns are being modified. For example, when the HR. SALARY table is SELECTED using direct database connection (not from the application), a condition could be to log the details of result sets where the PROPOSED_SALARY column is greater than \$500,000 USD.
5. **Redo log data** – Database redo log file data. The redo log files store all changes that occur in the database. Every instance of an Oracle database has an associated redo log to protect the database in case of an instance failure. In Oracle Audit Vault, the capture rule specifies DML and DDL changes that should be checked when Oracle Database scans the database redo log. (Micheal A.Miller, 2016)

4.4 Access Control

The P4 of the audit will be Access Control. Access controls is one of the major components of the database security. There are several access control policies that can be found in auditing. The three major classes of the policies can be grouped as: Discretionary access control (DAC), Mandatory access control (MAC) and Role-Based access Control (RBAC). DAC are those policies which are based on the identity of the person who requests it and on access rules what requestors are (or not) allowed. MAC policies are slightly different from the DAC in which the central authority is the head and it make sure to mandated regulations in access control. Finally, RBAC policies of access control totally depend on the roles that what users are in the system and what rules are stating for what accesses are allowed and disallowed to users (Yang, 2009).

In this research we have found two more important sub parts of access control for the betterment of IT Audit Quality which are stated as: **Database Physical Security** and **Database Logical Access**.

Access controls are basically those procedures, statements and policies that are made to allow data processing assets only with the management's authorization. Physical and logical access controls basically is used to protect the important assets which are not be used by unauthorized users and prevent from happening any damage, loss or modification. The data processing which is needed to be protected are system software, history files, and transaction detail and application programs with tables. Access to these files should be given only to authorized users to maintain a system.

4.5 Alerts, Report and IT Audit Quality information

The P5 and one of the most important audit process is the IT audit quality. The audit reporting which is installed by default is shown as follows –

1. Activity Reports
2. Entitlement
3. Stored Procedure Audit
4. Alerts

This is the list of audit report installed (Micheal A.Miller, 2016).

Table 4.1: Audit Reports

Type	Report	Description
Activity	Activity Overview	Digest of all captured audit events for a specified period of time
Activity	Data Access	Details of audited read access to data for a specified period of time
Activity	Data Modification	Details of audited data modification for a specific period of time
Activity	Data Modification Before-After Values	Details of audited data modifications for a specified period of time showing before and after values
Activity	Database Schema Changes	Details of Audited DDL activity for a specific time

The audit quality and the activities that are shared in these reports are of many importance. Thus, these reports are part of the IT Audit which will change the quality of the Audit as it should be. The report consists of many important types like Activity Overview, Data Access, Data Modification etc. These reports have genuine reason to react with the quality of audit which is taken place in the database. So, to digest all the events that are being captured by these activities for a specific period of time will ensure that the quality of audit is low, neutral or high.

4.6 Summary

The above sections of this chapter have described in detail the five factors (constructs) that have the most influence on the quality of database security audit process to derive to the proposed conceptual model of this project. With the proposed model, the relevant data is gathered from the survey participants in which these data will subsequently be analyzed to come up with the results of this project which will be discussed and concluded in the next chapters of this report.

CHAPTER 5

FINDINGS AND ANALYSIS

5.1 Introduction

The following chapter present the result of the statistical analysis findings in the proposed study. The data analysis is based on the collected data from the staff of IT and Database Centre in CICT (UTM). The validation done in this chapter has been made by comparison method. The ISDAA framework has been compared with some previous frameworks in this chapter to build and enhanced framework.

5.2 Validation Technique 1: Comparison against other models

The objective of this first validation, *Comparison against other models*, is to identify *any missing concepts* in the initial version of the metamodel and to also ensure its broad coverage. In this technique, concepts of the framework are validated and compared against concepts of other (valid) existing similar domain models or frameworks. The goal of the information security database audit and assessment framework is to express how the various models or frameworks have been tested. Specifically, Database security framework will be used to generate all concepts in the initial framework. The initial framework contains 7 frameworks as shown in Figure

2.4 This is a selection of frameworks that were chosen from previous frameworks and their components led to a framework which is known as the initial stage or the version 1.1 framework.

The comparison of the initial framework with other frameworks will ensure that if there is any change needed in the current framework or not. The process of the initial framework was simple and elegant and can be approached by a UTM CICT datacenter staff member. This evolution of ISDAA ensures that its semantics are sufficiently rich and broad. It ascertains that Database security audit can represent the variables of the frameworks from table 2.4. As described earlier, this version 1.1 is a collection of database security audit frameworks that represents different perspectives on the Information security audit domain. Database security audit will be modified to ensure that every framework in this set can be represented.

5.2.1 v1.1: Against the Challenges of Data Quality and Assessment in Database (LiCai, 2015)

This assessment is a database quality analysis framework which to process the quality of big data in database systems. In different business environments, the selection of data quality elements will differ. For example, for social media data, timeliness and accuracy are two important quality features. However, because it is difficult to directly judge accuracy (Shankaranarayanan, Ziad, & Wang, 2012), some additional information is needed to judge the raw data, and other data sources serve as supplements or evidence. Therefore, credibility has become an important quality dimension. However, social media data are usually unstructured, and their consistency and integrity are not suitable for evaluation. However, due to the lack of uniform standards, data storage software and data formats vary widely. Thus, it is difficult to regard consistency as a quality dimension, and the needs of regarding timeliness and completeness as data quality dimensions are not high. These require the data to comply with specific conditions or features. The formulation of assessment indicators also depends on the actual business environment.

Each quality dimension needs different measurement tools, techniques, and processes, which leads to differences in assessment times, costs, and human resources. In a clear understanding of the work required to assess each dimension, choosing those dimensions that meet the needs can well define a project's scope. The preliminary assessment results of data quality dimensions determine the baseline while the remaining assessment as a part of the business process is used for continuous detection and information improvement.

After the quality assessment preparation is completed, the process enters the data acquisition phase. There are many ways to collect data (Zhu & Xiong, 2009), including: data integration, search-download, web crawlers, agent methods, carrier monitors, etc. The IT Audit quality and the measured data quality assessment is almost like each other regarding the improvement of the quality of the assessment. Whereas, the access control is kind of like formulating evaluation baseline and can be compared. As usual in the end all the process has to have a result and report. So both the frameworks have 3 components that are very similar to each other.

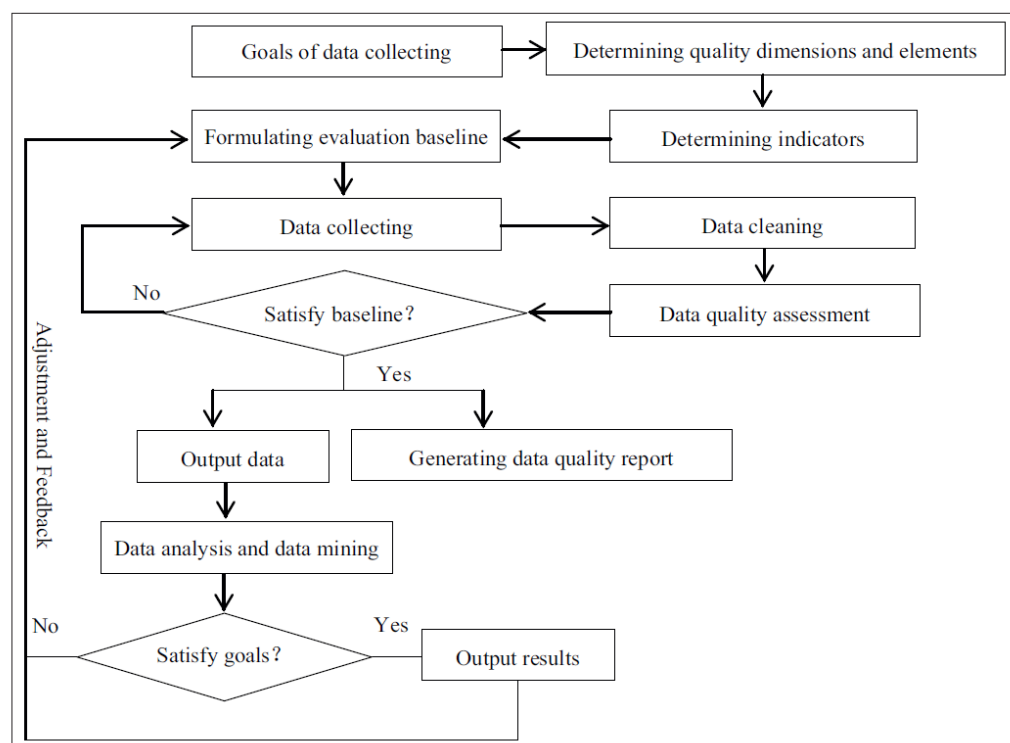


Figure 5.1: Quality audit assessment of Big Data in Database (LiCai, 2015)

Table 5.1: Quality assessment of big data support concepts in Database security audit framework

Against Concept	Variables Definition	ISDAA Concept	ISDAA Definition
Data Quality Assessment	Data quality assessment is to assess the quality of the data whether by qualitative method or quantitative method	IT Audit Quality	IT audit quality is basically used to have a good throughout quality of the database audit.
Output results	The output results will be the final answer to the process	Results and alerts	Results and analysis is the final result of the whole audit process.
Formulating Evaluation Baseline	Formulating the baseline of the process is to start the process from the best possible way and collect the data. Without the baseline you are restricted to start the process.	Access Control	Access Control is the selective restriction to a place or other source.

5.2.2 v1.2: Against Integrity Framework for Database Auditing (Michael A.Miller, 2016)

Databases nowadays are a very critical substance which every organization must protect for the sake of their private records. Integrity database log and audit framework is basically used of the Oracle Audit Vault and it can also be used for Database Firewall (AVDF). The Oracle AVDF is basically a simple tool which is mainly used for the database logging and auditing and the framework basically provides a methodology which if implemented can be applied to all the databases under Oracle AVDF (Michael A.Miller, 2016)

Table 5.2: Integrity Framework for database auditing Concept supports the ISDAA Concept

Against Concept	Variables Definition	ISDAA Concept	ISDAA Definition
Native Auditing	Native audit is a term for tools and resources that enable administrators to conduct an internal audit of database activity. Conventional relational database management systems come with these types of auditing tools, to allow for better protection of the data that gets entered into the systems.	IT Audit Quality	IT audit quality is basically used to have a good throughout quality of the database audit.
Reporting	The output results and reporting are the final part of the audit	Results and alerts	Results and analysis is the final result of the whole audit process.
Protected Audit Data	The data which is protected either physically or logically in a database when it is being audited is called Protected Audit Data.	Access Control	Access Control is the selective restriction to a place or other source.

5.2.3: V1.3: Against Overview of Database Auditing Framework (Oracle.com, 2010)

Managers have realized that the information gleaned from audit trails of database activity can be the company's single largest data resource. They also recognize that their audit trails provide a temporal 'third dimension' of their information, a valuable time-series view of their production systems that contains all-important behavioral aspects of their data access. While there are various approaches to auditing critical database platforms, implementing an enterprise class solution that provides a comprehensive auditing and reporting capability is not an easy task. We'll begin with a summary of the most important concerns of the IT manager and then examine various methods of implementing a successful enterprise auditing solution.

The main points of this framework address the issues of the highest concern for IT management.

1. Avoiding business risk and meeting the demands of customers and business partners: While the laws demand a thorough and comprehensive approach to privacy and auditing, the most important reason for protecting your data integrity is your professional reputation. The standards are high, and it is necessary to have a complete top-down auditing and protection solution to work with other businesses. Your partners must cover themselves and they are not likely to have the time, money or patience to audit a complicated home-grown solution. Remember, the driving force is your business need and your customer demand for data integrity and privacy.
2. Satisfying the auditors: Implementing best practices including segregation of duties: When considering the Build vs. Buy approach, it should be carefully

considered that systems administrators, database administrators and developers cannot have direct access to the auditing solution because exposures result when they have intimate knowledge of the internals of the audit mechanism. Any auditing solution must have the capability of providing for segregation of duties to ensure that these users can be denied access to the resulting audit trail to ensure the integrity of audit reports generated by the system.

3. Avoiding civil and criminal penalties - Data asset management practices must address business, operational, legal and compliance needs. Many Federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes Oxley Act (SOX) and the Gramm Leach Bliley Act (GLBA) change the way that databases are secured and audited and some of these federal regulations impose severe criminal penalties for non-compliance and malfeasance with protected data. Non-compliance with these regulations can also expose your company to multi-million-dollar civil lawsuits from customers if their private information has been improperly disclosed.

4. Choosing the right auditing approach: Many database vendors (e.g., Microsoft, Oracle) offer product-specific utilities to enable auditing, but these audit and trace tools are generally meant to be used only sporadically for investigative and forensic activity. Piecemeal solutions to auditing are difficult to scale, generally impose significant performance impact on the systems, and are very difficult to manage. Approaching auditing and privacy efforts at the application layer leaves direct access to the database unaudited, and results in incomplete coverage and a hodge-podge of in-house and third-party audit logs that are impossible to manage and reconcile.

These are just a few of the IT managers' concerns in this brave new world of security, privacy and regulatory compliance. Your customers and business partners

expect you to have a complete privacy auditing solution. Let's take a closer look at the issues and see how you can protect yourself from common pitfalls and implement a comprehensive and manageable solution. In this framework we can see that SQL and Oracle are the two main things that are being compared by with the initial framework. Object DDL will come in both oracle database as well as in SQL.

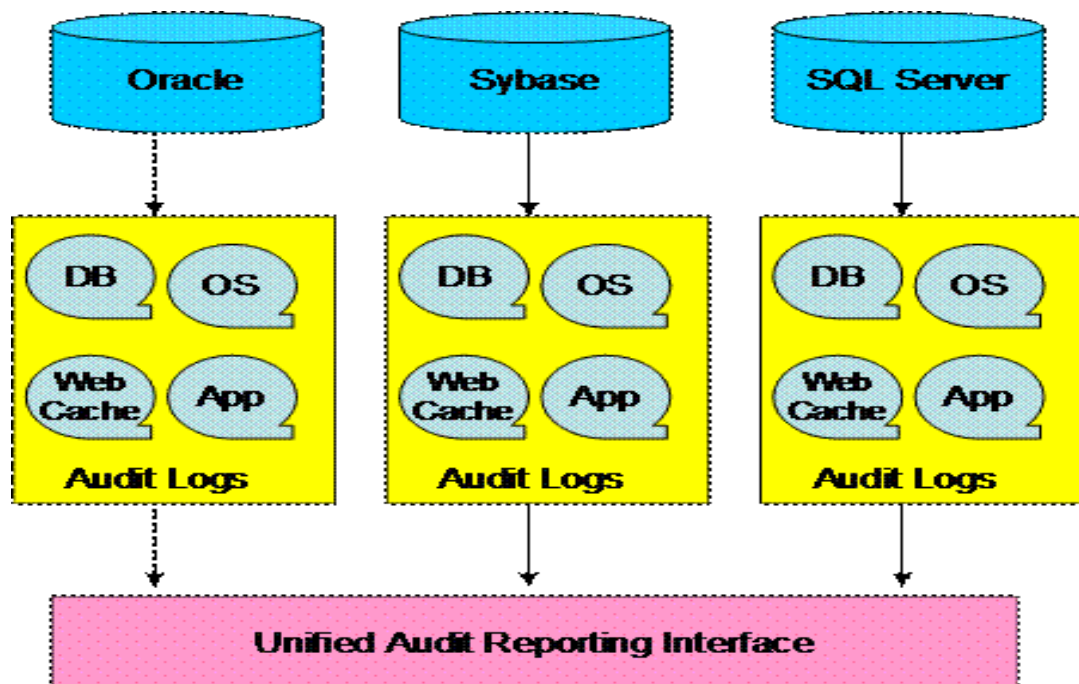


Figure 5.3: Overview of database auditing framework (Oracle.com, 2010)

Table 5.3: Overview of database auditing framework concept support the ISDAA concept

Against Concept	Variables Definition	ISDAA Concept	ISDAA Definition
SQL	SQL is an abbreviation for structured query language, and pronounced either see-kwell or as separate letters. SQL is a standardized query language for requesting information from a database	SQL(DML)	DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: <i>SELECT</i> , <i>UPDATE</i> , <i>INSERT</i> statements. In this the statements which are given above will be created once the audit of the database is done.
Oracle	Oracle database (Oracle DB) is a relational database management system (RDBMS) from the Oracle Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users (or an application front end) through structured query language (SQL).	Oracle Database Control	Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment and manages some large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivering is in high performance.
Sybase	Sybase was an enterprise software that produced software to manage and analyze information in relational databases.	Object(DDL)	A data definition language or data description language (DDL) is syntax similar to a computer <u>programming language</u> for defining <u>data structures</u> , especially <u>database schemas</u> . In the auditing phase of the database this command comes under the standard oracle auditing and is basically to create and alter the objects.

5.2.4: V1.4: Against A Framework for Database Audit and Control Flow Checking for a Wireless Telephone Network Controller

The proposed framework provides high modularity and transparency allowing for easy extensibility of the audit subsystem. New error detection and recovery

techniques can be implemented, encapsulated in new elements, and added to the system. A new element to be incorporated into the system needs to define and communicate to the audit main thread a set of messages that the element is capable of processing. The different audit elements can be quite independent of each other, which allows for easy customizability of the audit subsystem. Information security database audit and assessment (ISDAA) framework when compared to this framework it classifies that the database audit has a DB client which is also called Database Client and with that we have Audit Interference in which there are several parts such as Audit elements, Static and dynamic data check, Database API and many more. Audit Elements is compared to IT Audit Quality in figure 5.4 because IT Audit Quality also concern with all the quality and Audit elements.

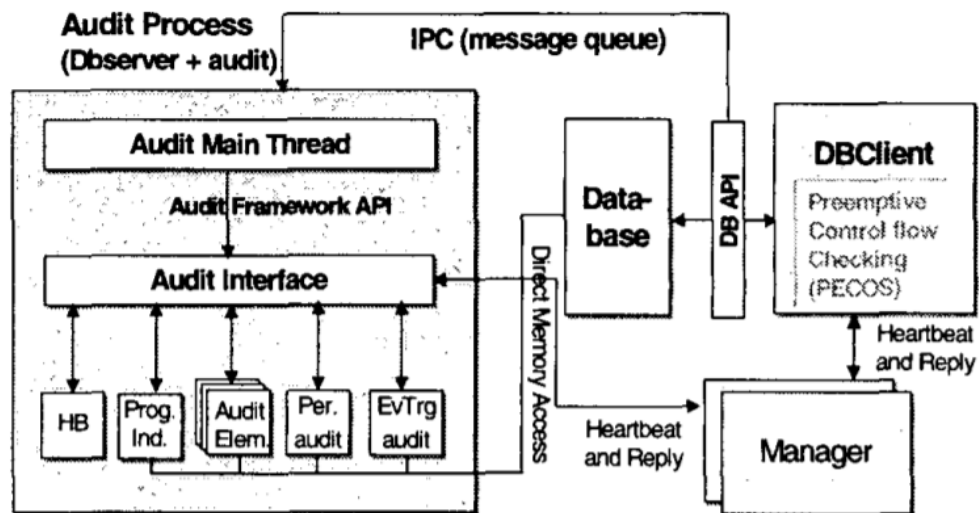


Figure 5.4: Audit process (S. Baghchi, 2000)

Table 5.4: Database audit framework for control flow support concept of ISDAA

Against Concept	Variables Definition	ISDAA Concept	ISDAA Definition
Database (SQL)	SQL is an abbreviation for structured query language, and pronounced either see-kwell or as separate letters. SQL is a standardized query language for requesting information from a database	SQL(DML)	DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: <i>SELECT</i> , <i>UPDATE</i> , <i>INSERT</i> statements. In this the statements which are given above will be created once the audit of the database is done.
Audit Elements	Specific audit techniques are implemented as separate audit elements in the audit process. The invocation of the audit elements can be either by a periodic trigger, or by an event trigger. The periodic trigger is based on a fixed time period. The event trigger is provided by some specific database operations, e.g., database write in the current implementation. The periodic audit element uses as its basis the periodic heartbeat query discussed earlier as trigger to perform the following audits: static data integrity check, dynamic data range check, structural audit, and referential integrity audit	IT Audit Quality	Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment and manages some large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivering is in high performance.

5.2.5: V1.5: Against a practical database framework for intrusion detection system

The DIDS proposed above is not just a monitoring tool. It can record all the communication packets between the client and the database. As we know, DBMS provides the audit capability, which could affect the efficiency of the data management. Therefore, the DIDS could take the task of auditing and alleviate the burden of the DBMS. We can make use of other professional data mining tools to exploit and audit the logs made by the DIDS. Finally, the DIDS is not under just passive detection mode but also could take some measures to prevent the intrusion if

necessary. The component of the Protection Proxy installed in the database host could receive commands from the DIDS Analyzer & Controller to adopt strategies to protect the database, such as killing database sessions or restarting server processes. As you can see in figure 5.5 you will clearly see that SQL and Oracle databases are similar to the ISDAA framework. The rest of the components are not so much related to ISDAA framework components. Access Control and Object DDL will also be used in it.

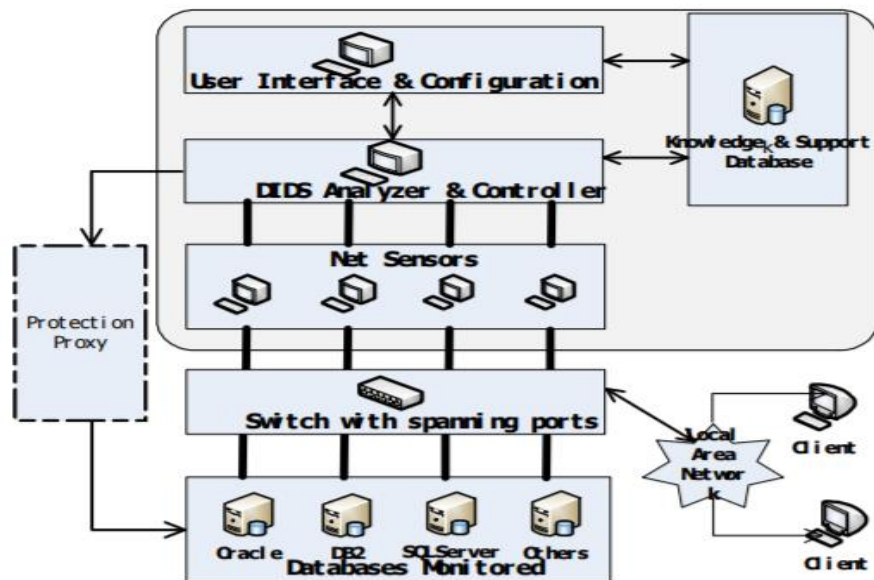


Figure 5.5: Deployment of the DIDS

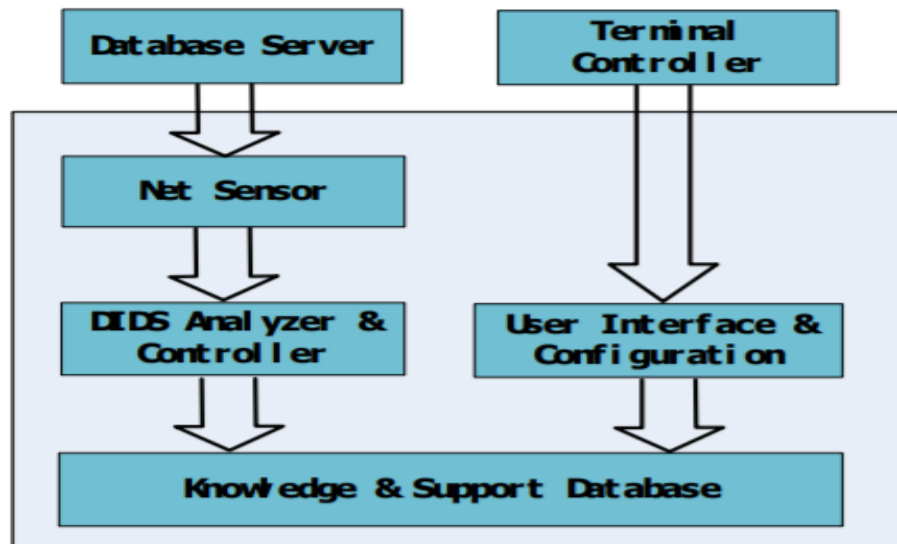


Figure 5.6: Architecture of the DIDS

Table 5.5: Database framework IDS support concept of ISDAA

Against Concept	Against Definition	ISDAA Concept	ISDAA Definition
Oracle	Oracle database (Oracle DB) is a relational database management system (RDBMS) from the Oracle Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users (or an application front end) through structured query language (SQL).	Oracle Database Control	Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment and manages some large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivering is in high performance.
SQL	SQL is an abbreviation for structured query language, and pronounced either see-kwell or as separate letters. SQL is a standardized query language for requesting information from a database	SQL(DML)	DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: <i>SELECT</i> , <i>UPDATE</i> , <i>INSERT</i> statements. In this the statements which are given above will be created once the audit of the database is done.

Oracle	Use same Oracle definition as mentioned Above	Object (DDL)	A data definition language or data description language (DDL) is syntax similar to a computer <u>programming language</u> for defining <u>data structures</u> , especially <u>database schemas</u> . In the auditing phase of the database this command comes under the standard oracle auditing and is basically to create and alter the objects.
User Interface and configuration	The User Interface & Configuration provides visual interfaces for end users, including receiving configuration commands from end users to reconfigure the DIDS Analyzer & Controller, allowing end users to define their own intrusion detection rules and so on.	Access Control	Access Control is the selective restriction to a place or other source.

2.5.6: v1.6: Against Database Auditing for Oracle Database

In addition to these economic losses or the status of the organization is damaged or breached can result into governing fines and a lot of fees would have to be paid for this. Thus, every organization needs to protect their valuable data as well as their databases. Database auditing involves monitoring and recording which can be made for only selected user database actions, so they can be aware what actions have the users got. Some of the security databases are shown below (ElhamIskandarnia, 2013).

The auditing concept is basically for the prevention and the threats to be detected. Nowadays many of the organization are facing the same problems that is the security of their databases and are also realizing that how to recognize a threat and then treat that threat in a cost-effective manner. This audit concept will basically help the University-Based Organization to minimize the cost of the database security (Reena R. Chaudhari, 2015).

The conceptual framework for this is that the tools for the auditing is used by DBA and examines the locations where databases stores auditing records, and study the actions produced by Database Management System (DBMS) as well as add actions to satisfy the requirements. In this framework we will see that figure 5.7 shows the tools that are used to audit databases in Oracle. In this framework almost all of the variables of ISDAA and the other framework are supported.

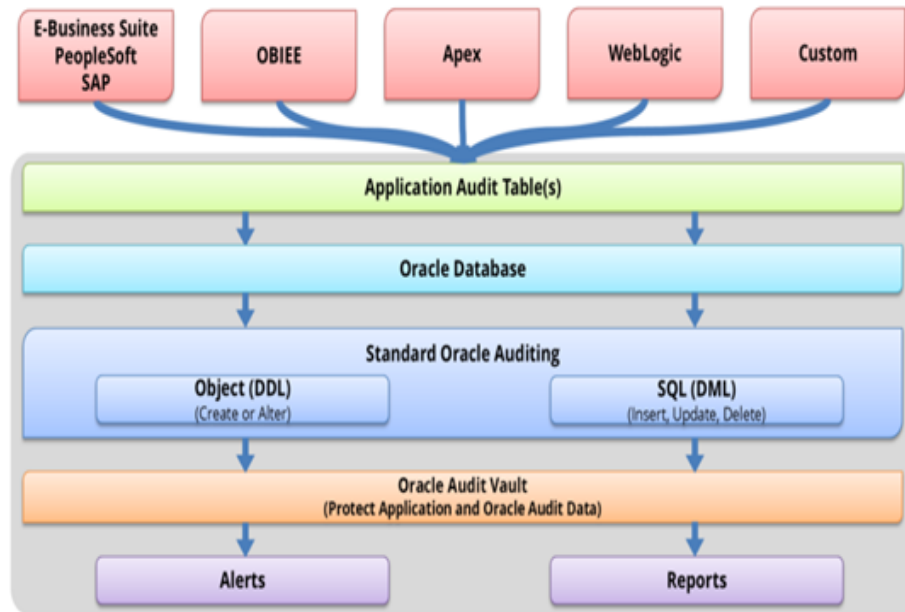


Figure 5.7: Integrity Framework for auditing and logging for database (Micheal A. Miller, 2016)

Table 5.6: A comparison between Integrity Framework concept and ISDAA concept

Against Concept	Against Definition	ISDAA Concept	ISDAA Definition
Oracle Database Control	Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment	Oracle Database Control	Database controls are basically designed to ensure that all the security, integrity, accountability of the database is in well controlled. Information Management has many problems. So, the key to finding these problems is Database servers. In general, a server basically involves some multiuser environment and manages some large amount of data so that the users can control the data

	and manages some large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivering is in high performance.		easily. All this of these things will be accomplished if the delivering is in high performance.
SQL(DML)	DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: <i>SELECT</i> , <i>UPDATE</i> , <i>INSERT</i> statements. In this the statements which are given above will be created once the audit of the database is done.	SQL(DML)	DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. Examples: <i>SELECT</i> , <i>UPDATE</i> , <i>INSERT</i> statements. In this the statements which are given above will be created once the audit of the database is done.
Object(DDL)	A data definition language or data description language (DDL) is syntax similar to a computer <u>programming language</u> for defining <u>data structures</u> , especially <u>database schemas</u> . In the auditing phase of the database this command comes under the standard oracle auditing and is basically to create and alter the objects.	Object (DDL)	A data definition language or data description language (DDL) is syntax similar to a computer <u>programming language</u> for defining <u>data structures</u> , especially <u>database schemas</u> . In the auditing phase of the database this command comes under the standard oracle auditing and is basically to create and alter the objects.
Reports and alerts	Results and analysis is the final result of the whole audit process.	Reports and alerts	Results and analysis is the final result of the whole audit process.

5.3 Comparing concepts in frameworks of V1 against ISDAA Concepts

Table 5.7: Comparing concepts in frameworks v1 against ISDAA concepts

Model in V1 set	Its ISDAA Support	ISDAA Lack of Support	ISDAA modification
V1.1,	<ul style="list-style-type: none"> - Data Quality Assessment (IT Audit Quality) - Output results (<i>Results and output</i>) - Formulating Evaluation Baseline (Access Control) 	Alerting	- Add "Alerting"
		Monitoring	- Add "Monitoring"
V1.2,	<ul style="list-style-type: none"> - Native Auditing (IT Audit Quality) - Reporting (<i>Results and Alerts</i>) - Protected Audit Data (<i>Access Control</i>) 	- DB Log Files	- Add: "DB Log Files"
V1.3 ,	<ul style="list-style-type: none"> - Oracle (Oracle Database Control) - Sybase (Object DDL) - SQL(SQL DML) 	All Supported	No
V1.4,	<ul style="list-style-type: none"> - Database (SQL DML) - Audit Elements (IT Audit Quality) 	DB Client DB API	- Add "DB Client" - Add "DB API"
V1.5,	<ul style="list-style-type: none"> Oracle (Oracle Database Control) SQL (SQL DML) Oracle (Object DDL) User Interface and 	All-supported	No

	Configuration (Access Control)		
V1.6,	- Oracle Database Control (Oracle Database Control) - SQL(DML) (SQL DML) - Object (DDL) (Object DDL) - Reports and Alerts (Reports and alerts)	All-supported	No

5.4 Expert Reviews and justification of the enhanced framework

In the content validity case, the proposed study was sent to experts to be validated. The survey instruments were modified based on the comment of the experts. Data centre experts were very important in this part of the validation because their comments matter a lot. Table 5.8 will show the expert review interview about the initial and enhancement of the framework.

Table 5.8: Expert Reviews

Experts	Asked Questions	Review
CICT Database Administrator	Q-1: Is the Components in the initial framework applicable in the CICT database centre? Q-2: After Comparison of the previous framework with the ISDAA framework the results of enhancement are 7 more components which are DB log, DB Client, Data	A1: Yes, the components of the initial framework is good for the Database Center. A2: The enhancement of components after the validation by comparison is ok. But Data Mining, Syslog and Quality Dimensions and elements cant be part of the

	<p>Mining, Quality Dimensions and elements, Syslog, DB API and Alerting and Monitoring.</p> <p>Q-3: In the end the enhanced framework is applicable for Datacenter of CICT when audit is being done?</p>	<p>enhancement only the remaining ones like DB Client, DB API, DB log and Alerting and Monitoring can be a part of the enhanced framework.</p> <p>A3: Yes the enhanced framework is now applicable for doing audit in datacenter of CICT.</p>
IT Department Head	<p>Q-1: Which type of Database do CICT use?</p> <p>Q-2: Does the database center have regular audits when the time is right?</p> <p>Q-3: Will this framework be helpful for auditing of database of CICT?</p>	<p>A1: They use both SQL and Oracle Databases.</p> <p>A2: Not always.</p> <p>A3: Yes it will be very helpful</p>

5.5 Enhanced Information Security Database Audit and Assessment Framework

This enhanced proposed framework will ease the staff to perform Database security process in more secure and sufficient manner. The enhancement saw 4 changes that are Database log (DB log), Database Client (DB Client), Alerting and Monitoring and Database API (DB API) which is made in the initial framework that was produced in Figure 4.1.

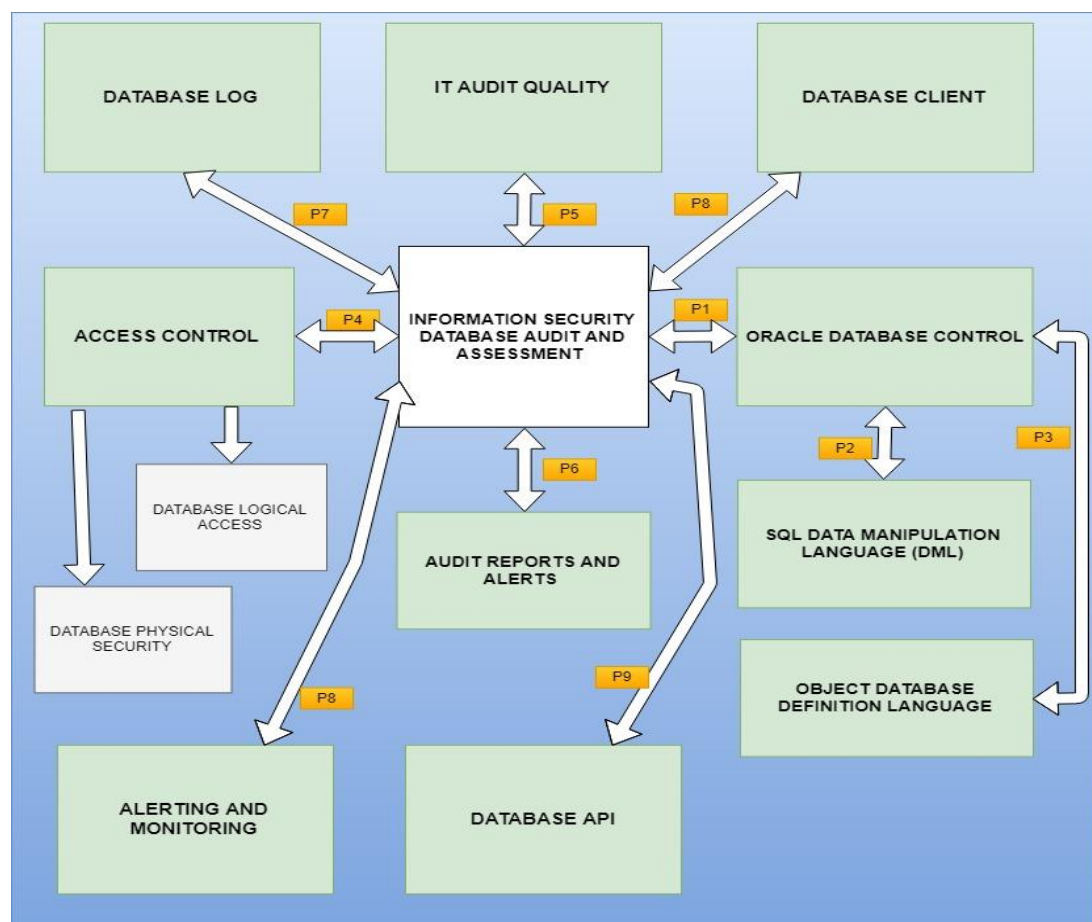


Figure 5.8: Enhanced Information Security Database Audit and Assessment Framework

Table 5.9 will show the Audit process that are shown in the Figure 5.8 and also there relationship with each other.

Table 5.9: Audit Process Relationship

Process	Relationship
P1	Oracle Database Controls – Information Security Database Audit and Assessment(ISDAA)
P2	SQL(DML)-Oracle Database Controls-ISDAA
P3	Object(DDL)-Oracle Database Controls-ISDAA
P4	Access Control- ISDAA
P5	IT Audit Quality- ISDAA
P6	Database Client (DB Client)-ISDAA
P7	Database Log (DB log)- ISDAA
P8	Alerting and Monitoring- ISDAA
P9	Database API (DB API)- ISDAA

The framework validation which is done by the comparison of the previous framework is taken in review by the experts to make sure that enhanced components are applicable or not. In that when the initial framework was validated by comparison with 6 previous frameworks it enhanced almost 7 components from which the Database Administrator rejected 3 and approved 4 when the expert review validation was done. So, the enhanced components and the rejected components are shown in Table 5.8.

5.6 Chapter Summary

This project has 5 variables that have previously discussed in chapter 4. In this chapter the results and findings for this research has been provided with help of comparison with 6 previous frameworks on Database security audit. Expert reviews were also taken from the database administrator of CICT in order to validate the enhanced components and make sure that the components are reliable for the Database audit of CICT or not.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Introduction

This chapter recapitulated and illustrates the achievement, limitations and challenges as well as future work of the research project. The proposed framework is of information security of database audit and its assessment. This project research will ensure the audit quality of the databases used in university organization environment. This research project aimed to have good quality of the audit for the databases and some knowledge to the users and staff as well that how we can secure the databases. Besides, this security of database audit framework desired to define the protection of data assets and to improve the audit quality.

6.2 Overview

This chapter reviews and concludes the entire study of the project. The more concern of this research project is to classify the achievements boundaries and the future improvements in the proposed Framework of information security of database audit and assessment. Thus, security framework aims to help the database users in accomplishing the awareness of incident related to the quality of the audit. The

proposed security framework will help identifying threats and their impact that causes to reveal the confidential data assets in the database.

Another hand, this research project will provide a solution to minimize or reduce risks that can lead to destroying important information assets that are reserved in the database. Besides, this research will discuss about the accomplishments in this project and, same time to reviews the finding. Moreover, this project highlighted the strengths and the challenges been faced in this project research and then the further project will be highlighted in this chapter.

6.3 Project Achievement

The achievements in this study are achieved by the three objectives that are mentioned in the first chapter.

6.3.1 Framework for Information Security database audit and assessment

The second objective was achieved by framework that contains three components which responds the security of database and the audit quality. Critical analysis was utilized in the proposed framework of database audit for managing the process of assessing the audit quality in the secure manner. Moreover, each of the framework components has critically analyzed. Finally, the draft of the proposed framework of database audit and assessment in university organization has designated and then perfectly designed.

6.4 Project Shortcomings and Constraints

The shortcomings and challenges that were faced during the course of this research include the following:

- i. At the initial state of this research the author finds it hectic to analyze the existing works and how to figure out the research gap,
- ii. The number of respondents that used to fill the questionnaires were limited due to the numbers of university staff members,
- iii. Installation of the SPSS software was difficult to manipulate and the use of the software itself was hard to understand and
- iv. The hardware equipment of the simulation was hard to manipulate.

6.5 Concluding Remarks

Chapter 1 has shown the background of the information security database audit which include the definition, problems and issues. Also shows the aim of study for this research which is to determine the level of information security database audit quality among staff members in UTM (CICT). The objectives of this research as well as the project scopes are identified as a guideline for this research.

Chapter 2 shown several research discussed about the audit quality for a database system and also the audit components that showed that how the process of audit is taken place which include: 1) Preparation, 2) Performance, 3) Reporting and 4) Conclusion. The detailed understanding of the existing works is important to identify the problems and issues in current content assess.

Chapter 3 serves the purpose for the details of the processes which are carried out to complete and fulfill the research objectives for this research project regarding information security database audit and assessment. This chapter shows that the process are distributed into 3 main phases which in detail describes how this project

will work and the details of this phases are given in a systematic way. The research framework will determine how the process will work in this project.

Chapter 4 of this research is the sections of this chapter that have described in detail the five factors (constructs) that have the most influence on the quality of database security audit process to derive to the proposed conceptual model of this study. With the proposed model, the relevant data is gathered from the survey participants in which these data will subsequently be analyzed to come up with the results of this study which will be discussed and concluded in the next chapters of this report.

Chapter 5 of this research has 5 variables that have previously discussed in chapter 4. In this chapter the results and findings for this research has been provided with help of comparison with 6 previous frameworks on Database security audit.

6.5 Summary

This chapter explains what have been covered and the objectives that were achieved in this research. The primary goal of this research was achieved by proposing framework of information security database audit and assessment. The proposed framework is to manage the quality of audit for databases in university organization. The proposed framework has been successfully validated by the respondent's university CICT staff members and upper management of the database systems. This framework can be very helpful to all database systems and their users. Finally, all objectives were achieved with less hindrance and future work has been outlined in this chapter.

REFERENCES

- A. Da Veiga, J. E., 2010. A framework and assessment instrument for information security culture. pp. 196-207.
- Anon., 2014. K. Wu, L. Hua, X. Wang and X. Ding. In: *The design and implementation of database audit system framework*. s.l.:Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS, pp. 553-556.
- Archives, 2017. Identifying Information Assets and Business Requirements. In: s.l.:s.n.
- Brad Tuttl, S. D. V., 2007. An empirical examination of COBIT as an internal control framework for information technology.
- Davis, C. S. M. & Wheeler, K., 2010. IT Auditing. In: *IT Auditing*. s.l.:s.n., pp. 394-397.
- ElhamIskandarnia, 2013. Database Autopsy Close Look to Database Auditing for Oracle Database. In: s.l.:Global Journal of Computer science and technology.
- Fielden, K., 2010. Information Security Framework. pp. 25-30.
- Gail Ridley, J. Y. P. C., 2004. COBIT and its Utilization: A framework from the literature. *The Hawaii International Conference on System Sciences*.
- Gusti Ayu, S. I. P. A. B., 2014. Governance Audit of Application Procurement Using COBIT Framework.
- Jia Shi, J. Y. M. L., 2016. Research on Database Audit Scheme Design of Life Insurance Industry Based OLAP Technology. *IEEE*.
- Kehe Wu, L. H. ,. X. W. X. D., 2014. The design and implementation of Database Audit system framework. pp. 553-556.
- L. Liu, Q. H., 2009. A Framework for database auditing. In: s.l.:ICCIT 2009- 4th Int. Conf. Comput. Sci. Converg. Inf. Technol, pp. 982-986.
- Lianzhong Liu, Q. H., 2009. A Framework for Database Auditing. *International Conference on Computer Science and Convergence Information Technology*, pp. 982-986.
- Micheal A.Miller, S. K., 2016. Integrity Guide to Oracle Audit Vault. In: s.l.:s.n.

O. Cinar, R. H. G. a. A. Y., 2017. Database Security in Private Database Clouds. In: s.l.:ICISS 2016 Int. Conf. Inf. Sci. Secur.

Reena R. Chaudhari, D. J. W. B., 2015. Overview of Database Auditing for Oracle Database. In: s.l.:International Journal of Application or Innovation in Engineering and Management, pp. 189-196.

Rouse, M., 2013. *Data and data management*. [Online]

Available at: <http://whatis.techtarget.com/definition/information-assets>

[Accessed 20 November 2017].

Russel, J., 2013. What is auditng?. In: s.l.:s.n.

Russell, J., 2013. *What Is Auditing*, USA: ASQ Quality Press.

Yang, L., 2009. Teaching Database Security and Auditing. *Department of Computer Science and Engineering Universty Of Tennessee*, pp. 241-245.

APPENDIX A

COMPARISON TABLE OF FRAMEWORKS

Model in V1 set	Its ISDAA Support	ISDAA Lack of Support	ISDAA modification
V1.1,	<ul style="list-style-type: none"> - Data Quality Assessment (IT Audit Quality) - Output results (<i>Results and output</i>) - Formulating Evaluation Baseline (Access Control) 	Alerting	- Add "Alerting"
		Monitoring	- Add "Monitoring"
V1.2,	<ul style="list-style-type: none"> - Native Auditing (IT Audit Quality) - Reporting (<i>Results and Alerts</i>) - Protected Audit Data (<i>Access Control</i>) 	- DB Log Files	- Add: "DB Log Files"
V1.3 ,	<ul style="list-style-type: none"> - Oracle (Oracle Database Control) - Sybase (Object DDL) - SQL(SQL DML) 	All Supported	No
V1.4,	<ul style="list-style-type: none"> - Database (SQL DML) - Audit Elements (IT Audit Quality) 	DB Client DB API	<ul style="list-style-type: none"> - Add "DB Client" - Add "DB API"

V1.5,	Oracle (Oracle Database Control) SQL (SQL DML) Oracle (Object DDL) User Interface and Configuration (Access Control)	All-supported	No
V1.6,	- Oracle Database Control (Oracle Database Control) - SQL(DML) (SQL DML) - Object (DDL) (Object DDL) - Reports and Alerts (Reports and alerts)	All-supported	No